[4910-15-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

United States Coast Guard

33 CFR Parts 101, 103, 104, 105, 106, 125

46 CFR Parts 10, 12, 15

49 CFR Parts 1515, 1570, 1572

[Docket Nos. TSA-2006-24191; USCG-2006-24196]

RIN 1652-AA41

Transportation Worker Identification Credential (TWIC) Implementation in the Maritime Sector; Hazardous Materials Endorsement for a Commercial Driver's License

AGENCY: Transportation Security Administration; United States Coast Guard, DHS.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: This is a notice of proposed rulemaking by the Department of Homeland Security, specifically by the Transportation Security Administration and the United States Coast Guard. If promulgated, this rule would implement the Transportation Worker Identification Credential program in the maritime sector. Under this program, merchant mariners holding an active License, Merchant Mariner Document, or Certificate of Registry and workers who require unescorted access to secure areas at maritime facilities or on vessels must undergo a security threat assessment, and, if found to not pose a security threat, obtain a Transportation Worker Identification Credential.

Persons without Transportation Worker Identification Credentials will not be granted unescorted access to secure areas at affected maritime facilities or on vessels.

Under this proposed rule, the Coast Guard seeks to amend its regulations on vessel and facility security to require the use of the Transportation Worker Identification Credential as an access control measure. It is also proposing to amend its regulations covering merchant mariners to incorporate the requirement to obtain a Transportation Worker Identification Credential. In a separate rulemaking action published elsewhere in this edition of the Federal Register, the Coast Guard also is proposing to consolidate existing licensing and documentation regulations to minimize duplicative or redundant identification or background check requirements.

The Transportation Security Administration proposes amending its security threat assessment standards that currently apply to commercial drivers authorized to transport hazardous materials in commerce to also apply to merchant mariners and workers who require unescorted access to secure areas on vessels and at port facilities. These proposed amendments also relate to the notification an employer receives when an employee who holds a hazardous materials endorsement or a Transportation Worker Identification Credential is determined to pose a security threat. The Transportation Security Administration also is proposing regulations dealing with the enrollment of port workers into the Transportation Worker Identification Credential program.

In addition, the Transportation Security Administration is proposing a fee, as authorized under the Department of Homeland Security Appropriations Act of 2004, to pay for the costs related to the issuance of the Transportation Worker Identification Credentials under this rule.

This rulemaking would enhance the security of ports by requiring background checks on persons and establishing a biometric access control system to prevent those who pose a security threat from gaining unescorted access to secure areas of ports. This rulemaking implements the Maritime Transportation Security Act of 2002, which requires that credentialed merchant mariners and workers with unescorted access to secured areas of vessels and facilities be subject to a security threat assessment and receive a biometric credential needed to access secured areas.

DATES: Comments and related material must reach the Docket Management Facility on or before [Insert date 45 days after date of publication in the Federal Register]. Comments sent to the Office of Management and Budget (OMB) on collection of information must reach OMB on or before [Insert date 45 days after date of publication in the Federal Register].

PUBLIC MEETINGS: TSA and the Coast Guard will hold four public meetings as follows: Wednesday, May 31, 2006 in Newark, NJ; Thursday, June 1 in Tampa, FL; Wednesday, June 6 in St. Louis, MO; and Thursday, June 7 in Long Beach, CA. Interested individuals are invited to attend, provide comments and ask questions about the proposed rule. TSA and Coast Guard will provide exact locations and other additional information about the meetings in another Notice to be published in the Federal Register.

ADDRESSES: You may submit comments identified by TSA docket number TSA-2006-24191 or Coast Guard docket number USCG-2006-24196 to the Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

(1) Web site: http://dms.dot.gov.

(2) Mail: Docket Management Facility, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street SW, Washington, DC 20590-0001.

(3) Fax: 202-493-2251.

(4) Delivery: Room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

(5) Federal eRulemaking Portal: http://www.regulations.gov.

You must mail comments on collection of information to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW, Washington, DC 20503, ATTN: Desk Officer, United States Coast Guard.

See SUPPLEMENTARY INFORMATION for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT:

For questions related to TSA's proposed standards: Rick Collins, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220, TWIC Program, 571-227-3515; e-mail: credentialing@dhs.gov.

For legal questions: Christine Beyer, TSA-2, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; telephone (571) 227-2657; facsimile (571) 571 1380; e-mail Christine.Beyer@dhs.gov.

For questions concerning the Coast Guard provisions of this proposed rule: LCDR Jonathan Maiorine, Commandant (G-PCP-2), United States Coast Guard, 2100 Second Street, SW, Washington, DC 20593; telephone 1(877) 687-2243.

For questions concerning viewing or submitting material to the docket: Renee V. Wright, Program Manager, Docket Management System, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street SW, Washington, DC 20590-0001; telephone (202) 493-0402.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to http://dms.dot.gov and will include any personal information you have provided. We have an agreement with the Department of Transportation (DOT) to use the Docket Management Facility. Please see DOT's "Privacy Act" paragraph below.

Submitting comments: If you submit a comment, please include your name and address, identify the docket number for this rulemaking (TSA-2006-24191 or USCG-2006-24196), indicate the specific section of this document to which each comment applies, and give the reason for each comment. Please send comments on the TSA portions of the proposed rule to the TSA docket (TSA-2006-24191), and send comments on the Coast Guard portions of the proposed rule to the Coast Guard docket (USCG-2006-24196). You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under ADDRESSES; but please submit your comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like us to acknowledge receipt, please enclose a stamped, self-addressed postcard or envelope.

We will consider all comments and material received during the comment period. We may change this proposed rule in view of them.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments: Do not submit comments that include trade secrets, confidential commercial or financial information, or sensitive security information (SSI)[1] to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the TSA legal point of contact listed in the FOR FURTHER INFORMATION CONTACT section.

Upon receipt of such comments, TSA will not place the comments in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold them in a separate file to which the public does not have access, and place a note in the public docket that TSA has received such materials from the commenter. If TSA receives a request to examine or copy this information, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's FOIA regulation found in 6 CFR part 5.

Viewing comments and documents: To view comments, as well as documents mentioned in this preamble as being available in the docket, go to http://dms.dot.gov at any time, click on "Simple Search," enter the last five digits of the docket number for this rulemaking, and click on "Search." You may also visit the Docket Management Facility

[1] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

in Room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

Privacy Act: Anyone can search the electronic form of all comments received into any of our dockets by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). You may review the Department of Transportation's Privacy Act Statement in the Federal Register published on April 11, 2000 (65 FR 19477), or you may visit http://dms.dot.gov.

Abbreviations and Terms Used in This Document

AMS—Area Maritime Security

ASP—Alternative Security Program

ATSA—Aviation and Transportation Security Act

ATF – Bureau of Alcohol, Tobacco, Firearms, and Explosives

CDC—Certain Dangerous Cargo

CDL—Commercial drivers license

CDLIS—Commercial drivers license information system

CHRC—Criminal history records check

CJIS—Criminal Justice Information Services Division

COR—Certificate of Registry

COTP—Captain of the Port

DHS—Department of Homeland Security

DOJ—Department of Justice

DMV—Department of Motor Vehicles

DOT—Department of Transportation

FBI—Federal Bureau of Investigation

FIPS 201—Federal Information Processing Standards Publication 201

FMCSA—Federal Motor Carrier Safety Administration

FMSC—Federal Maritime Security Coordinator

FSP—Facility Security Plan

HME—Hazardous materials endorsement

HSA—Homeland Security Act

HSPD 12—Homeland Security Presidential Directive 12

ICC—Integrated Circuit Chip

MARSEC—Maritime Security

MMD—Merchant Mariner Document

MSC—Marine Safety Center

MTSA—Maritime Transportation Security Act

OCS—Outer Continental Shelf

REC—Regional Exam Center

SAFETEA-LU - Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users

STCW—International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers, 1978, as amended

TSA—Transportation Security Administration

TWIC—Transportation Worker Identification Credential

USA PATRIOT Act— Uniting and Strengthening America by

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

VSP—Vessel Security Plan

Table of Contents

33 CFR Part 101

33 CFR 101.105 Definitions.

33 CFR 101.121 Alternative Security Programs—TWIC Addendum.

33 CFR 101.514 TWIC Requirement.

33 CFR 101.515 Personal identification.

33 CFR Part 103

33 CFR 103.305 Composition of an Area Maritime Security (AMS) Committee.

33 CFR 103.505 Elements of the Area Maritime Security (AMS) Plan and 103.510 Area Maritime Security (AMS) Plan review and approval.

33 CFR Part 104

33 CFR 104.105 Applicability.

33 CFR 104.106 Passenger Access Area.

33 CFR 104.115 Compliance dates.

33 CFR 104.120 Compliance documentation.

33 CFR 104.200 Owner or Operator/104.210 Company Security Officer (CSO)/104.215 Vessel Security Officer (VSO)/104.220 Company or vessel personnel with security duties/104.225 Security training for all other personnel

33 CFR 104.235 Vessel recordkeeping requirements.

33 CFR 104.265 Security measures for access control.

33 CFR 104.290 Security incident procedures.

33 CFR 104.295 Additional requirements—cruise ships.

33 CFR 104.405 Format of the Vessel Security Plan (VSP).

New Subpart E (33 CFR 104.500 – 104.510).

33 CFR Part 105

33 CFR 105.115 Compliance dates.

33 CFR 105.120 Compliance documentation.

33 CFR 105.200 Owner or operator/105.205 Facility Security Officer (FSO)/105.210 Facility personnel with security duties/105.215 Security training for all other facility personnel.

33 CFR 105.225 Facility recordkeeping requirements.

33 CFR 105.255 Security measures for access control.

33 CFR 105.280 Security incident procedures.

33 CFR 105.285 Additional requirements-passenger and ferry facilities.

33 CFR 105.290 Additional requirements-cruise ship terminals.

33 CFR 105.295 Additional requirements-Certain Dangerous Cargo (CDC) facilities.

33 CFR 105.296 Additional requirements-barge fleeting facilities.

33 CFR 105.405 Format and content of the Facility Security Plan (FSP).

New Subpart E (33 CFR 105.500 – 105.510).

33 CFR Part 106

33 CFR 106.110 Compliance dates.

33 CFR 106.115 Compliance documentation.

33 CFR 106.200 Owner or operator/106.205 Company Security Officer (CSO)/106.210 OCS Facility Security Officer (FSO)/106.215 Company

or OCS Facility personnel with security duties/106.220 Security training for all other OCS facility personnel.

33 CFR 106.230 OCS facility recordkeeping requirements.

33 CFR 106.260 Security measures for access control.

33 CFR 106.280 Security incident procedures.

33 CFR 106.405 Format and content of the Facility Security Plan (FSP).

New Subpart E (33 CFR 106.500 – 106.510).

Miscellaneous Items.

33 CFR 101.305 (Reporting requirements).

33 CFR 101.400 (Enforcement)

33 CFR 104.130, 105.130, and 106.125 (Waivers).

33 CFR Subpart C Parts 104,105, and 106 (Security Assessments).

46 CFR Parts 10, 12, and 15.

VI. Section-by-Section Analysis of TSA Proposed Rule

49 CFR Part 1515 Appeal and Waiver Procedures for Security Threat Assessments for Individuals.

49 CFR 1515.1 Scope.

49 CFR 1515.3 Terms used in this part.

49 CFR 1515.5 Appeal procedures.

49 CFR 1515.7 Waiver Procedures.

49 CFR Part 1570 Land Transportation Security: General Rules.

49 CFR 1570.3 Terms used in this part.

49 CFR Part 1572 Credentialing and Background Checks for Land Transportation Security.

49 CFR 1572.5 Scope and standards for hazardous materials.

49 CFR 1572.7 Waivers of security threat assessment standards.

49 CFR 1572.9 Applicant information required for security threat assessment for a hazardous materials endorsement.

49 CFR 1572.11 Applicant responsibilities for a security threat assessment for a hazardous materials endorsement.

49 CFR 1572.13 State responsibilities for issuance of hazardous materials endorsement.

49 CFR 1572.15 Procedures for security threat assessment for an HME.

49 CFR 1572.17 Applicant information required for the security threat assessment for TWIC.

49 CFR 1572.19 Applicant responsibilities for a security threat assessment for TWIC.

49 CFR 1572.21 Procedures for security threat assessment for a TWIC.

49 CFR 1572.23 Conforming Equipment; Incorporation by reference.

49 CFR 1572.24-40 [Reserved]

49 CFR 1572.41 Compliance, inspection and enforcement.

49 CFR 1572.101 Scope.

49 CFR 1572.103 Disqualifying Criminal Offenses.

49 CFR 1572.105 Immigration status.

49 CFR 1572.107 Other analyses.

L. Technical Standards

M. Environment

VIII. List of Subjects

IX. The Amendments

I. Background and Purpose

Under this rule, the Department of Homeland Security (DHS), through the United States Coast Guard (Coast Guard) and the Transportation Security Administration (TSA), proposes to require that all merchant mariners holding an active License, Mechant Mariner Document, or Certificate of Registry and all persons who need unescorted access to secure areas of a regulated facility or vessel must obtain a Transportation Worker Identification Credential (TWIC). In order to obtain a TWIC, individuals will be required to undergo a security threat assessment conducted by TSA. TSA, in conducting those security threat assessments, will use the procedures and standards established by TSA for commercial motor vehicle drivers licensed to transport hazardous materials within the United States.

The implementation of the TWIC program in the maritime sector builds upon existing Coast Guard credentialing requirements and security programs for port facilities and vessels. In a separate rulemaking action published in this issue of the Federal Register, Coast Guard also proposes consolidating existing merchant mariner licensing and documentation requirements to avoid duplicative credentials and background checks and to avoid interruption in commerce and reduce the burden on mariners.

The TWIC program is a DHS initiative, with joint participation of the Coast Guard and TSA. The program is supported by several statutory and regulatory

authorities and presidential directives. The principal statutory authority is the Maritime Transportation Security Act (MTSA), Pub. L. 107-295, 116 Stat. 2064 (November 25, 2002) (46 U.S.C. 70105). Section 102 of MTSA requires the Secretary of Homeland Security to issue a biometric transportation security credential to merchant mariners "issued a license, certificate of registry, or merchant mariners document" and individuals who require unescorted access to secure areas of vessels and facilities.[2] These individuals also must undergo a security threat assessment to determine that they do not pose a security threat prior to receiving the biometric credential and authority to access the secure areas without escort. Id. The security threat assessment must include a review of criminal, immigration, and pertinent intelligence records in determining whether the individual poses a threat, and individuals must have the opportunity to appeal an adverse determination or apply for a waiver of the standards. Specifically, an individual cannot be denied the transportation security credential required under MTSA unless the individual—

(A) Has been convicted within the preceding 7-year period of a felony or found not guilty by reason of insanity of a felony—

(i) that the Secretary believes could cause the individual to be a terrorism security risk to the United States; or

(ii) for causing a severe transportation security incident;

(B) Has been released from incarceration within the preceding 5-year period for committing a felony described in subparagraph (A);

[2] 46 U.S.C. 70105. Section 102 of MTSA defines "Secretary" to mean "the Secretary of the department in which the Coast Guard is operating." Under the Homeland Security Act of 2002, the Coast Guard became part of DHS, thus the Secretary of Homeland Security is authorized to implement the credential requirements for mariners and persons seeking access to secure port facilities under MTSA.

(C) May be denied admission to the United States or removed from the United States under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.); or

(D) Otherwise poses a terrorism security risk to the United States.

46 U.S.C. 70105(c).

Following the enactment of MTSA in November 2002, the Coast Guard issued a series of general regulations for maritime security. See, 33 CFR parts 101-106. The MTSA regulations set out specific requirements for owners and operators (henceforth "owners/operators") of vessels, facilities, and Outer Continental Shelf (OCS) facilities that had been identified by the Secretary of Homeland Security as posing a high risk of being involved in a transportation security incident.

Under MTSA and the Coast Guard's MTSA regulations, owners/operators of these vessels and facilities were required to conduct security assessments of their respective vessels and facilities, create security plans specific to their needs, and submit the plans for approval to the Coast Guard by December 31, 2003. All affected vessels and facilities are required to have been operating in accordance with their respective plans since July 1, 2004, and are required to resubmit plans every 5 years.

Each plan requires owners/operators to address specific vulnerabilities identified pursuant to their individual security assessments, including controlling access to their respective vessels and facilities. The MTSA regulations require owners/operators to implement security measures to ensure that an identification system was established for checking the identification of vessel and facility personnel or other persons seeking access to the vessel or facility.

In establishing the system, owners/operators were directed to accept identification only if it: 1) was laminated or otherwise secure against tampering; 2) contained the individual's full name; 3) contained a photo that accurately depicted that individual's current facial appearance; and 4) bore the name of the issuing authority. See, 33 CFR 101.515. The issuing authority must be a government authority or organization authorized to act on behalf of the government authority, or the individual's employer, union, or trade association. There was no requirement that the identification be issued pursuant to a security threat assessment because there was no existing credential and supporting structure that could fulfill the needs specific to the maritime environment.

In addition to the regulation of ports and facilities, the Coast Guard has a long history of regulating the merchant marine. Under the current Coast Guard regulatory scheme, the Coast Guard may issue a mariner any combination of 4 credentials: (1) Merchant Mariner Document (MMD); (2) License; (3) Certificate of Registry (COR); or (4) International Convention on Standards of Training, Certification, and Watchkeeping (STCW) Endorsement. An MMD serves as a mariner's identification credential and is issued to mariners who are employed on merchant vessels of 100 gross register tons or more, except for those vessels employed exclusively in trade on the navigable waters of the U.S. Licenses are qualification certificates that are issued to officers. CORs are qualification certificates that are issued to medical personnel and pursers. STCW Endorsements are qualification certificates issued to mariners who meet international standards and serve aboard vessels to which STCW applies. The License, COR, and STCW Endorsement are qualification credentials only. Only the MMD is an identity

document, and none of the current mariner credentials contain the biometric information required under MTSA.

TSA currently administers several programs involving security threat assessments of individuals engaged in the transportation industry, including certain airport and aircraft operator employees, and alien flight school students. Section 1012 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) Pub. L. 107-56, 115 Stat. 272 (October 25, 2001) provides that a State cannot issue a hazardous materials endorsement (HME) to a commercial driver who poses a security threat. TSA implemented its security threat assessment processes under this provision.

TSA first issued regulations to implement security threat assessment standards for HME applicants (TSA's hazmat rule) in May 2003 and subsequently amended those regulations based on comments received from the States, employers and affected drivers. (A more detailed discussion and regulatory history of the hazmat regulations can be found at 68 FR 23852 (May 5, 2003); 68 FR 63033 (November 7, 2003); 69 FR 17696 (April 6, 2004); and 69 FR 68720 (November 24, 2004). These standards are codified at 49 CFR part 1572, where many of the standards we propose for TWIC under this rule also will reside.

TSA's hazmat regulations establish standards concerning criminal history, immigration status, mental capacity, and terrorist activity to determine whether a driver poses a security threat and is qualified to hold an HME.[3] Drivers who have been convicted or found not guilty by reason of insanity for certain crimes in the preceding 7 years, or have been released from incarceration for those crimes in the preceding 5 years,

are deemed to pose a security threat and are not authorized to hold an HME. 49 CFR 1572.103. Drivers convicted of certain particularly heinous crimes, such as espionage, treason, terrorist-related offenses, or severe transportation security incidents, are permanently banned from holding an HME. Id. In addition, drivers who have been involuntarily committed to a mental institution or adjudicated as mentally incapacitated are considered to pose a security threat that warrants disqualification from holding an HME. 49 CFR 1572.109.

Aliens are not prohibited from obtaining an HME. The hazmat rule permits individuals who are in the United States lawfully and are authorized under applicable immigration laws to work in the United States to hold an HME upon completion of a satisfactory TSA security threat assessment. 49 CFR 1572.105. TSA reviews a driver's immigration status to determine if the applicant for an HME is authorized to be present and work in the United States under applicable immigration laws. In addition, as set forth in the hazmat rules, TSA conducts a security check of international databases through Interpol or other appropriate means. 49 CFR 1572.107.

TSA's hazmat regulations also include appeal and waiver procedures to ensure that no driver is wrongfully determined to pose a threat, to provide individuals who are disqualified from holding an HME the opportunity to show rehabilitation, where applicable, and to maintain consistency with other credentialing or background check requirements among transportation workers, such as those in the maritime industry covered by MTSA and this TWIC rulemaking. See e.g., 49 CFR parts 1572.141 and 143.

II. Development of TWIC Process

[3] In developing the hazmat regulations, TSA sought to harmonize, to the extent possible, the background

In 2002, TSA established the TWIC program in response to identity management shortcomings and vulnerabilities identified in the transportation system. In some segments of the transportation system, it is not possible to positively identify individuals entering secure areas or assess the threat they may pose due to a lack of pertinent background information. Also, existing identity credentials are often vulnerable to fraud. To mitigate these weaknesses, TSA determined that an integrated, credential-based, identity management system for all transportation workers who need unescorted access to secure areas of the nation's transportation system would be necessary.

Homeland Security Presidential Directive 12 (HSPD 12) requires Federal agencies to improve secure identification processes for Federal employees and contractors. The objectives of the directive are to ensure that the credentialing processes are administered by accredited providers; are based on sound criteria for verifying an individual's identity; include a credential that is resistant to fraud, tampering, counterfeiting and terrorist exploitation, and can be authenticated quickly and electronically. As designed and proposed in this rule, TWIC does not contradict the control objectives of HSPD 12

The U.S. Department of Commerce published guidance on the standards and methods by which Agencies could reach compliance with HSPD 12. In February 2005, the Department of Commerce issued the Federal Information Processing Standards Publication 201 (FIPS 201), Personal Identification Verification of Federal Employees and Contractors in response to HSPD 12. FIPS 201 is divided into Personal Identification Verification (PIV) Parts I and II. Part I addresses the control and security

---

check and eligibility criteria requirements of both MTSA and the USA PATRIOT Act and thus adopts

objectives, particularly the personal identity proofing process. Part II provides detailed technical specifications that must be met to ensure interoperability of PIV-compliant credentials in personal authentication, access control, and credential management systems throughout the Federal government.

The development of FIPS 201 occurred concurrently with the design of TWIC. TSA and its contractors closely monitored the development of FIPS 201 and individuals working on FIPS 201 followed the design of TWIC. TSA recognized that there are many benefits to designing TWIC in alignment with FIPS 201: leveraging the TWIC infrastructure to support other DHS or government credentialing programs; avoiding obsolescence by using the latest technology; securing critical facilities with the same process used by Federal agencies; having interoperability during an emergency; and demonstrating the functionality of FIPS 201. All of the significant components of the TWIC system align with FIPS 201.

As tested in the maritime environment and planned in this NPRM, TWIC is an identification credential containing numerous technologies to make it secure and tamper-proof. TWIC is a "smart" credential containing two electronic chips on which encoded data is stored to allow all subsequent TWIC functions to be performed. TWIC is designed to ensure that the identity of each TWIC holder has been verified; that a threat assessment has been completed on that identity; and that each credential issued is positively linked to the rightful holder through the use of biometric technology. Facility and vessel owners/operators subject to this rule will then determine which TWIC holders will be granted unescorted access to secure areas of their facility.

---

privisions from both statutes where appropriate. See 68 FR at 23853.

Prototype

The TWIC program has been developed in three phases. Phases I, Planning, and II, Technology Evaluation, were completed in 2003, and Phase III, Prototype, was completed in 2005. In the technology evaluation, TSA tested and evaluated a range of credential-based systems in use at transportation facilities. In Prototype, TSA tested a comprehensive credentialing system, which included enrollment, threat assessments, biometric security, credential production, and credential issuance.

Prototype was conducted at twenty-eight facilities beginning November 4, 2004 in various modes of the transportation system, including air, rail, and maritime. The Prototype Phase came to an end in the summer of 2005. During Prototype, the participating facilities and associated transportation workers voluntarily provided biographical and biometric identifiers. Participants provided appropriate identity verification documentation, such as a birth certificate, driver's license, government photo identification, or similar document. TSA conducted a name-based threat assessment using the biographic information provided, and utilized the biometric information to verify identity and determine whether an applicant had previously enrolled in the program. TSA did not use biometric information to complete a security threat assessment.[4] TSA will be using both biographic and biometric information to conduct the security threat assessment once TSA implements the full program. To verify an individual's identity during Prototype, TSA followed the U.S. Citizenship and Immigration Services Employment Eligibility Verification (Form I-9) process, commonly

[4] Florida law requires persons seeking access to certain port facilities within that State to submit fingerprints and other information to obtain a State-issued credential. During Prototype conducted in Florida, therefore, participants submitted fingerprints as required under State law and the State completed a

used by the federal government and industry in the hiring process. TSA tested the TWIC as positive identification for access to secure areas of participating transportation facilities.

By testing the integration of these components, TSA was able to assess the system's performance prior to deciding how the program should be implemented. Consequently, some processes that were tested in Prototype, such as "employer sponsorship," are not being proposed in this rule based on TSA's determination that the process did not add sufficient value or created operational difficulties that could not be resolved.

III. Proposed Rule

A. Coast Guard

In order to integrate TWIC into already existing security programs in the maritime environment, the Coast Guard must amend its maritime security regulations, found in 33 CFR Subchapter H. These changes will set performance standards for owners/operators of vessels, facilities, and Outer Continental Shelf facilities to meet when incorporating TWIC into their existing security programs.

The Coast Guard also must amend its regulations governing merchant mariners, found in 46 CFR parts 10, 12, and 15, in order to add the statutory mandate that they hold a TWIC. In a separate rulemaking, published in today's Federal Register, the Coast Guard is proposing to consolidate qualifications credentials and streamline its mariner regulations, which would ensure that no mariner is required to undergo (or pay for) more than one security threat assessment and identitiy verification.

---

fingerprint-based criminal history records check. TSA did not use biometric information collected from

Coast Guard emphasizes that possession of the TWIC credential is not intended to constitute an automatic access right to any facility. The owner/operator continues to have the ultimate authority as to access control decisions, and although holding a duly-issued TWIC is required before an individual is eligible to be granted unescorted access, the individual must also have a need for access in accordance with the approved security plan. The owner/operator's right to refuse admittance to any individual, regardless of whether he or she holds an authenticated TWIC, remains unchanged.

B. TSA

TSA's role in implementing the TWIC program in the maritime sector will be to conduct security threat assessments of credentialed merchant mariners and individuals with unescorted access to secure areas, providing an appeal and waiver process for applicants who receive an adverse determination, and performing related functions in the enrollment and credential issuance process. In this rule, TSA proposes changes to its regulations to extend the current processes for conducting security threat assessments for HMEs to persons seeking to obtain TWICs.

In August 10, 2005, the Safe, Accountable, Flexible, Efficient Transportation Equity Act—A Legacy for Users (SAFETEA-LU), Pub. L. 109-59, 119 Stat. 1144 (August 10, 2005) was enacted. Section 7105 of SAFETEA-LU (49 U.S.C. 5103a(g)(1)(B)(i)) requires TSA to initiate a rulemaking to determine which background checks required by Federal law and applicable to transportation workers are equivalent to or less stringent than the security threat assessment TSA requires for HME drivers. In addition, SAFETEA-LU requires TSA to develop

---

Florida participants to conduct a security threat assessment.

a process for notifying employers of the results of a threat assessment conducted on an HME applicant.

Under this rule, TSA is proposing a fee to cover the cost of the TWIC threat assessment, appeals of TSA decisions during the process, and the issuance of the credential as required under Section 520 of the Homeland Security Appropriations Act of 2004 (2004 DHS Appropriations Act), Pub. L. 108-90 (October 2003). TSA also is inviting comments from the transportation industry at large on the processes proposed under this rule as TSA and DHS are considering extending the TWIC program to other areas in the transportation industry outside of the maritime sector.

1. TWIC Process

As proposed in this rule, the purpose of the TWIC program is to ensure that only authorized personnel who have successfully completed a security threat assessment have unescorted access to secure areas of maritime facilities and vessels. The credential will include a reference biometric -- fingerprints -- that positively links the credential holder to the identity of the individual who was issued the credential. TWIC holders may be asked to confirm, by providing a fingerprint, that they are the rightful owner of the credential at any time. Access control procedures and systems at facilities and vessels will recognize the credential and the information encrypted on it, so that the overall maritime network will be interoperable. In addition, an individual's credential can be deactivated or revoked by TSA if disqualifying information is discovered by or presented to TSA or other DHS entity, or the credential is lost or stolen, so that the credential can no longer be used to obtain unescorted access to secure areas.

TSA has designed the TWIC process to maintain strict privacy controls so that a holder's biographic and biometric information cannot be compromised. The TWIC process proposed in this rule is described below from the perspective of an applicant.

a. Pre-Enrollment and Enrollment

TWIC enrollment will be conducted by TSA (or TSA's agent operating under TSA's direction). All enrollment personnel must successfully complete a TSA security threat assessment and receive a TWIC before they will be authorized to access documents, systems, or secure areas.

Facility and vessel owners/operators must notify workers of their responsibility to enroll, as well as the deadline for doing so. (The proposed implementation plan for enrollment is discussed in greater detail below.) Owners/operators must provide applicants enough lead time to enroll so that TSA has sufficient time to complete the security threat assessment and issue the credential before the access control procedures go into effect. Generally, owners/operators should give individuals at least 60 days notice to begin the process. TSA cannot guarantee that any threat assessment can be completed in less than 30 days, and therefore, owners/operators and applicants should make every effort to initiate enrollment in a timely fashion to prevent workers being denied access for non-compliance. TSA will provide owners/operators with locations for enrollment that they can then pass on to the workers (hereinafter referred to as applicants). For purposes of the NPRM, a list of potential enrollment center locations is provided on the TSA Web site (www.tsa.gov) to provide prospective owner/operators and applicants a general idea of the enrollment plan. This list is subject to change and TSA invites comment from affected parties on the potential enrollment locations.

Applicants will be able to "pre-enroll" online to reduce the time needed to complete the entire enrollment process at an enrollment center. For pre-enrollment, applicants need a computer with internet access. The applicant can access the TWIC Web site to provide personal information required for enrollment and select an enrollment center at which to complete enrollment. Data submitted by applicants via the Internet will be sent using Internet security protocols (i.e., SSL). All information provided is then stored in the TSA system, which encrypts and protects the data from unauthorized access. Applicants may schedule an appointment while on-line to complete the enrollment process, although appointments are not required at enrollment centers. The Web site will list the documents the applicant must bring to the enrollment center to verify identity. The convenience of pre-enrollment is a significant benefit for applicants and reduces strain on the enrollment centers. Applicants who pre-enroll must appear at enrollment centers to verify their identity, confirm that the information provided during pre-enrollment is correct, provide biometrics, and sign the enrollment documents.

At the enrollment center, applicants will receive a privacy notice and consent form, by which they agree to provide personal information for the security threat assessment and credential. (For applicants who pre-enroll, the privacy notice is provided with the application on-line, but the applicants must acknowledge receipt of the notice in writing at the enrollment center.) If an applicant fails to sign the consent form or does not have the required documents to authenticate identity, enrollment will not proceed. During Prototype, 96 percent of applicants appeared for enrollment with suitable identity verification documents. As TWIC is implemented, TSA and Coast Guard will make information available to affected workers in advance of enrollment so that all are aware

of what to bring to the enrollment center. This information will also be posted on the TSA/TWIC Web site at www.tsa.gov. All information collected at the enrollment center or during the pre-enrollment process, including the signed privacy consent form and identity documents are scanned into the TSA system for storage. All information is encrypted or stored using methods that protect the information from unauthorized retrieval or use.

At the enrollment centers, applicants must provide ten fingerprints and sit for a digital photograph. The fingerprints and photograph will be electronically captured at the enrollment center for use on the credential. Individuals must provide ten fingerprint images for use in completing the security threats assessment process. The credential itself will store two fingerprint templates, one of which is used as a reference biometric to verify identity. The entire enrollment record (including the 10 fingerprints) will be stored in the TSA system, encrypted and segmented to prevent unauthorized use. TSA will provide alternative procedures for enrollment centers to use for situations in which an applicant is unable to provide fingerprints.

The TWIC fee, which covers the complete cost of enrollment, threat assessment, and credential production and delivery, must be collected from the applicant at the enrollment center prior to the enrollment record being transmitted to the TSA system. The TWIC enrollment fee will be non-refundable, even if the threat assessment results in a TWIC not being issued.

Once all data and the fee are collected, the enrollment record is encrypted and electronically transmitted to the TSA system. The TSA system acknowledges receipt of the enrollment record, at which time all enrollment data is automatically deleted from the

enrollment workstation. Once the enrollment record is transmitted to the TSA system, personal information is stored only in the TSA system, and personal data is encrypted to very high standards before it is transferred or stored. If an enrollment center temporarily loses its internet connection, the enrollment data is encrypted and stored on the enrollment workstation, but only until an internet connection is restored.

During Prototype, the average time needed for an applicant who pre-enrolled to complete enrollment was 10 minutes, 21 seconds. It is expected that it will take approximately fifteen minutes to complete enrollment of applicants who do not pre-enroll.

TSA and Coast Guard currently envision a phased enrollment process based on risk assessment and cost/benefit analysis. Locations that are considered critical and provide the greatest number of individual applicants will be among the earliest enrollment sites. There are approximately 125 locations covering approximately 300 ports where TSA plans to enroll applicants, and we are in the process of rating each location against a variety of factors to assess criticality, population, and infrastructure. TSA and Coast Guard will work closely with the maritime industry to ensure that owners/operators and workers are given as much notice as is possible when a definitive enrollment schedule is selected. TSA and Coast Guard also are contemplating implementing a more flexible rollout, with anticipated dates to be announced by notices published in the Federal Register. (See the discussion of § 1572.19 below for additional information on timing of enrollment.) TSA plans to use a combination of fixed and mobile enrollment stations to make the enrollment process as efficient as possible for applicants and owners/operators.

b. Adjudication of Security Threat Assessment

Following enrollment, the TSA system sends pertinent parts of the record to various sources so that appropriate terrorist threat, criminal history, and immigration checks can be performed. When the checks are completed, TSA makes a determination on whether or not to issue a TWIC to the applicant and notifies the applicant.

If disqualifying information is discovered, TSA issues an Initial Determination of Security Threat to the applicant with information on how the applicant can appeal an adverse decision or apply for a waiver of the standards. If the applicant does not respond to the Initial Determination within a specified period, it converts to a Final Determination of Security Threat and the applicant does not receive a TWIC. If the applicant proceeds with an appeal or application for waiver and is successful, the applicant is notified accordingly and the credential production process begins. (The appeal and waiver processes are discussed in greater detail below in the section-by-section analysis.)

TSA may provide some of the notifications to applicants via email, if an applicant provides an email address on the application for the TWIC. We invite comment from prospective applicants about the substitution of email notification for a paper process.

c. Credential Production

If the applicant is qualified to receive a TWIC, the TSA system generates an order to produce a credential. It is produced at a government credential production facility and securely shipped to the center at which the applicant enrolled. The applicant will be notified that the TWIC is ready to be retrieved and activated for use. The face of the TWIC credential contains the applicant's photograph, name, TWIC expiration date, and a unique credential number. In addition, the credential will store finger minutia templates

of 2 fingers, finger pattern templates of 2 fingers, a personal identification number, and a Federal Agency Smart Credential number. The data is securely stored and protected in accordance with FIPS 201 in the various technologies used in the credential, such as magnetic stripe, contact chip, and contactless chip. The fingerprint data, the reference biometric, is used to match the credential to the person who enrolled.

The TWIC system contains many feedback mechanisms to validate the transmission and receipt of data at key points in the process. The status of each transmission is recorded within the system.

Credentials are electronically locked prior to shipment to the enrollment center so that the data cannot be accessed. Once the credentials are electronically locked, they cannot be used for access to any vessel or facility until they are activated by the TWIC enrollment station.

d. Credential Activation

The applicant is notified when the enrollment center has received the credential. The applicant then returns to the enrollment site at his or her convenience to activate the credential.

At the enrollment center, the applicant's credential is retrieved from secure storage and the photograph and name on it are compared to the applicant and the identity documents the applicant uses to authenticate identity. The applicant places a designated finger on a reader to generate a biometric match against the biometric stored on the credential and in the TSA system. Upon successful biometric match, the TWIC is activated and the applicant selects a Personal Identification Number (PIN) that also is stored on the credential. The PIN can subsequently be used as an additional factor in

proving one's identity and authorized use of the credential, or as the primary verification tool if the biometric is inoperative for some reason. The TWIC security threat assessment and credential are valid for five years, unless derogatory information is discovered and TSA revokes the credential.

The process outlined above for credential activation is the same process TSA tested in Prototype, which worked well for owner/operators and employees who enroll. However, implementation of the program nationwide involving employees that are not stationary at one facility or port may impact applicants and owner/operators differently. TSA is concerned that requiring an applicant to return to the enrollment center to activate the credential may be onerous for workers who travel a great deal and may not know where they will be when the credential is ready for pick-up. TSA is considering the security and operational impacts of alternative procedures, on which we invite comment.

TSA is considering an amendment to the process that would allow a worker to designate a specific enrollment center for credential pick up and activation. The card production facility would send the credential to that location rather than the location where the applicant enrolled. This is a change that can be accomplished, but this was not tested in Prototype and a variety of software changes may be needed, which could increase costs and affect the timing of implementation. Moreover, applicants will not know the exact date on which their credential will be ready and so those who work at a variety of ports across the country may not be able to designate a specific activation location on the enrollment application.

During Prototype, the entire process from enrollment to card production was complete in fewer than 10 days. However, that process differed from the full program we

plan to implement with this rule in a few significant ways. First, nearly all of the employees who volunteered for Prototype worked at the same location every day and the enrollment center was located on that site. Second, TSA did not complete fingerprint-based criminal history records checks, and so there was no time needed to adjudicate and provide redress for criminal activity. For threat assessment programs that are currently in place nationally in which applicants are not stationary and TSA conducts a fingerprint-based CHRC, the threat assessment is generally completed in less than 30 days. The time needed to complete the threat assessment varies depending on whether the database searches produce adverse information that must be investigated, and whether the applicant files an appeal or requests a waiver. These conditions will exist for the TWIC program and therefore, TSA will not be able to predict or establish a specific date on which the threat assessment and card production process will be complete.

DHS invites comment on this option, and any other proposals that would make it easier logistically, without sacrificing security, for the public to receive and activate TWIC cards.

e. Using TWIC in an Access Control System

Once the enrollment process is complete and the credential is activated, the credential is ready to be used as an access control tool. Possession of a TWIC does not guarantee access to secure areas because the owner/operator controls the individuals who are given unescorted access to the facility or vessel. Rather, TWIC is a secure, verified credential that can be used in conjunction with the owner/operator's risk-based security plan and as required by the Coast Guard security regulations.

As envisioned in this NPRM, owners/operators will determine an individual's need for unescorted access to secure areas and then grant access using a TWIC program. The access control administrator of the vessel or facility verifies that the individual holding the TWIC matches the biometric stored on the TWIC by conducting a 1-to-1 match with the individual's finger and the fingerprint template stored on the chip in the TWIC.

The owner/operator verifies that an individual's TWIC is valid, either by directly interfacing with the TSA system or by using a list of invalid credentials downloaded from TSA. Either method provides owners/operators pertinent information concerning the validity of the credential. TSA will invalidate credentials that are reported as lost, stolen, damaged, retired, or issued to an applicant that TSA subsequently determines may pose a security threat. When the invalidation is for cause, that is, due to a security threat, TSA will revoke the credential. Invalidated credentials cannot be used or honored for unescorted access to secure areas. Cardholders who report the credential as lost, stolen, or damaged must go to the enrollment center for resolution, and/or re-issuance of a new credential.

After the individual has been granted access to the facility, the owner/operator may opt to notify the TSA system that access privileges have been granted to this worker at that facility. If the owner/operator invokes this option, the owner/operator also assumes responsibility for informing the TSA system if the owner/operator subsequently denies the individual access privileges.

f. Lost, Damaged, or Stolen TWICs

Replacement TWICs are available if a credential is lost, stolen, or damaged. As soon as the applicant is aware that the credential is missing or damaged, he or she call the Call Center and the Center follows a standard process to invalidate the credential. The applicant then travels to an enrollment center to receive a new credential. During Prototype, the card production facility printed and shipped the new credentials within 24 hours of receiving the information. Applicants must pay a fee of $36 to cover the cost of lost/damage/stolen credential invalidation, new credential production, reissuance, shipping, and other appropriate program costs. No new TSA threat assessment-specific or enrollment costs are factored into this replacement fee.

g. Renewal

TWICs issued under this rule will expire after five years unless renewed. TSA does not plan to notify TWIC holders when their credential is about to expire because the expiration date will be displayed on the face of the credential. To renew a TWIC, the holder must appear at any enrollment center, starting up to 90 days before the expiration date of the credential, to initiate the renewal process. However, mariners are allowed and encouraged to initiate renewal 180 days prior to expiration to allow sufficient time for TSA to conduct the security threat assessment and the Coast Guard to complete any review necessary to renew any required mariner credentials. During renewal, applicants must provide the same biographic and biometric information required in the initial enrollment and pay the associated fees. A new credential is issued upon renewal.

h. Call Center

Upon publication of the final rule, TSA will refer the public to a Call Center to assist with questions about the TWIC program. An automated telephone line, listing options for the caller to select, will direct the caller to the TWIC Help Desk or the TSA/TWIC Web site. Callers will be able to discuss questions about the program and final standard, the status of their security threat assessment, the location and time of operation of enrollment centers, and online applications and educational materials. TSA has used the Call Center when implementing other new programs and believes it will be very useful to owners/operators and applicants.

i. Notifying Employers of Threat Determinations

TSA is proposing to modify the rule text applicable to HME applicants concerning employer notification and apply the proposed changes to the TWIC applicants.

As discussed above, SAFETEA-LU established several mandates concerning the threat assessment process. One of the provisions requires TSA to invite comment on and develop a process to notify employers of HME applicants of the results of the threat assessment. Specifically, section 7105 states that--

> Within 90 days of enactment, TSA, after receiving comments from interested parties, must develop and implement a process for notifying employers designated by applicants for a HAZMAT license of the results of the applicant's background check if (1) such notification is appropriate considering the potential security implications and (2) the Director determines in a final notification of threat assessment served on the applicant that he or she does not meet the standards for granting a license.

In the November 24, 2004 hazmat rule, TSA discussed employer notification, noting that actual criminal history or other dispositive records must be maintained confidentially by TSA. See 69 FR at 68726. TSA may inform an employer that an

employee is disqualified from holding an HME, or has had an HME revoked, so that the employer knows that the employee is not authorized to transport hazardous materials. TSA, however, generally cannot disclose the basis for the determination result of the threat assessment due to prohibitions on disclosure of such information under the Privacy Act, or other pertinent privacy laws or law enforcement or security regulations. See e.g., 5 U.S.C. 552a (as amended); 46 U.S.C. 70105(e); 28 CFR 50.12. In the hazmat rule, TSA noted that if it believes an immediate threat exists, TSA may provide additional information to the employer to help prevent a security incident.

In the November hazmat rule, TSA requested comment on methods to notify an employer that a particular driver's HME is revoked or the application for an HME is denied. TSA anticipated that it would be difficult to locate a driver's employer because drivers tend to change employers frequently and may work for several employers at one time. Also, many drivers are self-employed as owners/operators and notification in these cases would be unnecessary. TSA proposed requiring each employer to maintain a current list of hazmat-endorsed driver employees on a secure Web site that TSA could access for notification purposes and employers could amend as employees change jobs. This list would minimize the chance that TSA would erroneously notify a previous employer of a disqualification. Also, the list would prevent the loss of time and resources needed to locate an employer for notification. Similar procedures are in place with respect to aviation workers who have airport security identification display area authority. 49 CFR 1542.211. TSA received no comments on this proposal or suggestions for an alternative plan, although some employers stated that they would like notification of all employee disqualifications.

Currently, when TSA determines that a driver is not qualified to hold an HME, TSA applies the following policy:

(1) TSA notifies the employer only in cases where TSA determines that an imminent security threat may exist.

(2) TSA notifies the employer listed in the driver's HME application.

(3) TSA limits the information provided to the employer to the fact that the driver's HME is being revoked or denied, but does not provide the reason for the action.

TSA developed this process to address two primary concerns. First, TSA is concerned about sharing disqualification information with incorrect employers and that the likelihood of such notifications would rise if TSA made notifications in all disqualification cases. For the many drivers who change employers frequently or are self-employed, TSA would expend considerable resources trying to determine with certainty an applicant's current employer(s).

Second, for actions in which there is not an imminent threat, employers of hazmat drivers have other procedures in place to verify whether a driver has an HME. Carriers currently are required to determine if a driver employee has been issued an HME, by checking State driver records. The Federal Motor Carrier Safety Administration (FMCSA) requires carriers to check the driver's status in the first 30 days of employment by contacting the licensing State. After that, the carrier must make an inquiry with the State at least once annually to ensure that the driver is authorized to transport hazardous materials. 49 CFR 391.25. Additionally, FMCSA requires carriers to review an employee's driving record during the three years preceding employment with the carrier, in every State in which the driver was licensed. The carriers also must investigate the

driver's employment record during the preceding three years. 49 CFR 391.23. These investigations reveal whether the driver's HME has been revoked.

In light of the employer notification requirement in SAFETEA-LU, and upon further analysis, TSA proposes to amend the rule text concerning employer notification generally and apply the following proposed changes to HME and TWIC applicants. First, TSA proposes to add a statement to the application for an HME or TWIC acknowledging that TSA may notify the applicant's employer if TSA determines that the applicant poses a security threat. The applicant must acknowledge receipt of this statement. Second, TSA proposes to amend the rule text to state that TSA will notify an applicant's employer, where appropriate, when issuing final determinations of threat assessment or immediate revocations.

Aside from the employer notification issue, with TWIC applicants, TSA also proposes to notify the Federal Maritime Security Coordinator (FMSC), the chief governmental security official at the port, of revocations. The FMSC also is the Captain of the Port (COTP). 33 CFR 101.105. TSA will notify the Coast Guard concerning the outcome of threat assessments of merchant mariners because a mariner credential may not be issued by Coast Guard if TSA denies or revokes a TWIC for the mariner.

TSA invites comment on these proposed requirements for notifying employers of employee disqualifications. TSA also invites suggestions for improving this system and methods by which a current employer/employee list can be available to TSA when employer notification is necessary. TSA may change its requirements based on these comments.

2. Fee

Section 520 of the 2004 DHS Appropriations Act requires TSA to collect reasonable fees for providing credentialing and background investigations in the field of transportation. Fees may be collected to pay for the costs of the: (1) conducting or obtaining a criminal history records check (CHRC); (2) reviewing available law enforcement databases, commercial databases, and records of other governmental and international agencies; (3) reviewing and adjudicating requests for waivers and appeals of TSA decisions; and (4) other costs related to performing the security threat assessment or providing the credential or performing the background records check. Section 520 requires that any fee collected must be available only to pay for the costs incurred in providing services in connection with performing the security threat assessment or providing the credential or performing the background records check. The fee may remain available until expended. TSA establishes these fees in accordance with the criteria in 31 U.S.C. 9701 (General User Fee Statute), which requires fees to be fair and based on: (1) costs to the government, (2) the value of the service or thing to the recipient, (3) public policy or interest served, and (4) other relevant facts.

In this rule, TSA proposes to establish new user fees: (1) the Information Collection and Credential Issuance fee, estimated to range from $45 - $65; (2) the Threat Assessment and Credential Production fee, which will be $62, or $50 for applicants who have already received a comparable threat assessment from DHS, including those for a Merchant Mariner License (MML), Merchant Mariners Document (MMD), Hazardous Materials Endorsement (HME), and Free and Secure Trade (FAST) card holders; and (3) the fee for replacement of a lost. damaged, or stolen TWIC, which will be $36 for all

TWIC holders. In addition, TSA will collect the FBI Fee for the criminal history records checks in the TWIC threat assessment process and forward the fee to the FBI. The current FBI Fee is $22.00. If the FBI increases that fee in the future, TSA will collect the increased fee. Therefore, total TWIC fees are expected to range from $95 (MML, HME, and FAST card holders already vetted by DHS) to $149 for all other applicants.

3. TWIC in Other Modes of Transportation

This rule proposes standards for the maritime environment and consequently the security threat assessment standards primarily impact merchant mariners and port workers. However, there are a variety of individuals who work in other modes of transportation that may be subject to the security threat assessment requirement proposed here. For instance, many ports include railroad operations. Rail employees may be required to obtain a TWIC depending on whether the railroad operations are situated in the secure areas. Commercial truck drivers delivering or retrieving goods at the port typically have unescorted access to secure areas and so they would be required to have a TWIC. As envisioned and currently proposed in this rule, commercial drivers that hold an HME and have completed TSA's security threat assessment under 49 CFR part 1572 would not be required to undergo a new threat assessment for TWIC until their HME threat assessment expires. These drivers would be required to provide a biometric for use on the TWIC and pay for enrollment services, credential costs, and appropriate program support costs.

TSA is considering whether to incorporate the TWIC system into all modes of transportation. Therefore, TSA requests comments from all of the transportation industry--rail, mass transit, pipeline, and aviation--not just those affected immediately by

these specific proposed maritime rules. TSA invites ideas on how this security threat assessment and credentialing system can be used to its full potential in each of these areas. Each mode of transportation brings its own set of challenges to the philosophy of creating secure areas and access control procedures that provide a high level of security, protect privacy, and do not interfere with commerce. TSA welcomes the views of all interested parties as we continue to improve transportation security with TWIC and other programs.

IV. Advisory Committee Participation

In drafting the TWIC regulations, the Coast Guard drew upon the expertise of the National Maritime Security Advisory Committee (NMSAC), which is composed of a cross-section of maritime industries and port and waterway stakeholders; including, but not limited to: shippers, carriers, port authorities, and facility operators. NMSAC advises, consults with, and makes recommendations to, the Secretary of Homeland Security via the Commandant of the Coast Guard on matters affecting maritime security.

In response, NMSAC formed a Credentialing Work Group (CWG), which was comprised of a significant number of NMSAC members and approximately 25 other members from the public who represented various geographic cross-sections and different elements of the maritime industry. NMSAC provided the Coast Guard and TSA with specific industry sponsored comments and recommendations for consideration in developing this proposed rule. TSA and Coast Guard summarized these comments and provide their joint responses below.

A. Access Control

Comment: NMSAC recommended that "secure area" be defined to coincide with the access control area determined by the facility operator in its security plan.

Response: We agree with this recommendation and, for all of the reasons discussed in this NPRM, are including it in the Coast Guard's proposed definition of secure area.

Comment: NMSAC also recommended that when vessels are moored at MTSA regulated facilities, they should be allowed to rely on the facility's TWIC procedures and not be required to read an individual's TWIC again when he or she required unescorted access to the vessel from the facility.

Response: We agree with this recommendation in part. Nothing in the proposed rule prohibits vessels and facilities from agreeing to share the management of access control on a case-by-case or recurring basis to facilitate operations, subject to approval by the cognizant COTP. In keeping with the intent of MTSA, facilities and vessels will still retain ultimate responsibility for their own access control measures. In the interest of preserving layered security, we also anticipate there will be situations where persons seeking unescorted access should be required to follow access control procedures again—when moving from a vessel to a facility and vice versa—even if this requires repeating access control procedures.

Comment: NMSAC believes that TWIC should serve as the baseline requirement for unescorted access to a facility or vessel, allowing owners or operators to adopt additional measures.

Response: We agree with this recommendation. Nothing in this NPRM prevents an owner/operator from instituting additional requirements before granting access.

Comment: NMSAC also felt that possession of a TWIC should not guarantee access to a facility or vessel, or to a specific location within the site.

Response: We agree. Owners and operators decide who, among the TWIC holders, may have unescorted access to the facility or vessel.

Comment: NMSAC also recommended that access to Outer Continental Shelf facilities as defined in part 106, where access is limited and can be controlled by having the TWIC credential read at the point of embarkation.

Response: This arrangement is currently allowed under the existing regulations and could continue under the provisions of this NPRM.

B. Location of Reader Points

Comment: NMSAC recommends that the regulation not stipulate specific reader locations.

Response: We agree. Reader locations are not specified in the proposed rule. Owners/operators determine where readers are located, based on the security plan and the performance standards established in the NPRM.

Comment: NMSAC recommends that screening points should be placed far from critical areas and placement should be determined by owners/operators.

Response: Screening locations are not specified in the proposed rule. Owners/operators determine where screening points are located, based on the security plan and the performance standards established in the NPRM.

C. Sponsorship

Comment: A majority of NMSAC opposed employer sponsorship as a requirement of the TWIC application process. Many members believe sponsorship

introduced several complex components, including privacy concerns, increased bureaucracy associated with approving and monitoring sponsors, and employer liability issues.

Response: After careful consideration, we agree that sponsorship, as originally conceived, is a challenge for the maritime TWIC program. Many of the individuals who will require a TWIC, such as truck drivers and casual laborers entering the port, would not be able to list or obtain a sponsor. Making accommodations to the sponsorship process for these workers would greatly reduce its value. Under the NPRM, applicants are asked to provide information on their employer if applicable, and to certify that they have a need to obtain a TWIC.

D. Waiver Process/Alternative Security Arrangements

Comment: NMSAC recommended that we use the list of disqualifying offenses currently used for hazmat drivers for establishing disqualifying offenses, with some qualifications and concerns. The primary concern centered on the waiver requirements found in MTSA, which require employer involvement. NMSAC believes that employer involvement in the waiver process is inconsistent with MTSA's prohibition against disclosure of details of why an applicant is denied a TWIC. NMSAC recommended that the TWIC regulations rely upon the existing waiver procedures that apply to hazmat drivers.

Response: We agree. We have proposed using the same list of crimes currently in place under the hazmat regulations when making determinations regarding TWIC eligibility. Additionally, the NPRM contains the waiver procedures that currently apply to hazmat drivers.

Comment: NMSAC also expressed concerns about individuals currently employed in the maritime industry who might be denied a TWIC due to previous criminal activity. NMSAC believes existing employees should not be denied a TWIC and possibly lose their jobs unless TSA determines the individual to pose a risk based on the entire threat assessment. NMSAC recommended a "limited term waiver" that would allow an individual who is employed on the date of TWIC implementation, and is not otherwise determined to be a security threat, to obtain a TWIC.

Response: A "limited term waiver" is not being proposed. As in the hazmat rule, language in the waiver provisions of the NPRM allow individuals to request a waiver of all but four disqualifying offenses. These pertain to espionage, sedition, treason, and terrorism. In accordance with MTSA and the NPRM, individuals with immigration violations would also be ineligible for the TWIC. Under the hazmat program, the majority of workers with disqualifying offenses, other than those listed above, who have applied for a waiver have been successful in obtaining their endorsement through the existing waiver process. In addition, the time between publication of the final rule and the date an individual is required to obtain a TWIC will provide existing employees ample time to apply for a waiver.

Comment: NMSAC believes that the fingerprint data provided by applicants should be used to search all relevant federal databases. In addition, NMSAC suggested that TSA check against criminal databases in the applicant's State of residence. NMSAC also recommended that a nolo contendere plea be treated as a conviction.

Response: We intend to use an applicant's fingerprints to search the criminal databases that require fingerprints to gain access. However, there are some databases

pertinent to security that are accessed by name and therefore, we must use name and other biographic information to use these databases. Currently, we do not plan to check each State criminal database in addition to the FBI criminal databases. The administrative cost and time associated with such an undertaking would greatly increase the user fee and make adjudication of all applicant records overwhelming. Under this proposal, a nolo contendere plea constitutes a conviction.

Comment: NMSAC proposed that the regulations be consistent nationwide. NMSAC was concerned that if individual states are allowed to enact legislation that established standards different than the federal standard, it would result in additional costs and delays to the industry. NMSAC also believed that varied state background checks could result in venue shopping by applicants.

Response: We agree that the TWIC should be nationally consistent and that states do not have the authority to modify the federal TWIC program. However, States, when acting in their capacity as an owner or operator, retain the right of any owner or operator to impose additional security measures at their ports and facilities, as they see fit, including additional measures for access control beyond the TWIC requirements. In addition, States retain their sovereign police powers to impose statutes and regulations to protect their citizens from all manner of threats, and ensure public welfare. In that capacity, a State may impose additional measures at ports, facilities and vessels within its jurisdiction that are directed against reducing all types of crime, so long as those measures do not conflict with any existing Federal regulatory program or frustrate a Federal purpose, including the TWIC. Therefore, while the process for obtaining and maintaining a TWIC will be uniform across the country, access control measures may

vary across States, and even from facility to facility, which is in keeping with the recommendations of the NMSAC and the intent of this rulemaking.

E. Type of biometric to be used, other than fingerprints

Comment: NMSAC recommended that the applicant's digital photograph be stored on the integrated circuit chip (ICC) on the TWIC. Its format and technological standards should conform to other national and international programs, such as US-VISIT and FAST. NMSAC recommended that we reevaluate the use of fingerprint biometrics for access control after completion of Prototype to address procedures for individuals who cannot provide fingerprints.

Response: Regarding the first comment, we agree and are proposing that the applicant's digital photograph be stored within the TWIC's ICC. We agree with the second comment and are proposing a credential that meets or exceeds HSPD 12 and FIPS 201 technical standards, which are the baseline for all federal identification credentials. We also agree with the third comment and are proposing that the digital photograph be used as the alternate biometric for individuals who are unable to provide fingerprints at the time of issuance.

F. Federally-Managed vs. Federally-Regulated

Comment: NMSAC strongly supports a federally-managed approach to TWIC implementation, as opposed to a federally-regulated approach. NMSAC believes that a federally managed program would protect collective bargaining agreements, promote uniformity of process and technology, ensure appropriate auditing and oversight, protect the sensitivity of the biographic and biometric information required for application, and limit the potential for security compromises or other integrity issues. It also states that

there would be significant cost savings if TWIC is implemented in a centralized, federally managed program.

Response: We agree and the NPRM reflects this approach.

G. Enrollment

Comment: In the interest of time, NMSAC recommended that TSA provide as many enrollment centers as practical during the initial enrollment period, staffed either by DHS personnel or trained trusted agents. NMSAC believes that enrollment personnel should be subject to a higher level of scrutiny than TWIC applicants, including financial and credit screening. NMSAC recommended that TSA streamline the enrollment process by allowing pre-enrollment through secure Internet connections, dedicated kiosks, or existing facilities. NMSAC had reservations about allowing non-safety related agencies or organizations becoming involved in this process. They also recommend DHS first look to its own agencies, such as Coast Guard License Issuing Centers, or other federal, state or local public safety offices to process enrollments before seeking partnerships with agencies with non-security missions.

Response: We agree with most of the NMSAC recommendations. The current rollout strategy is phased enrollment over a period of time to accommodate the majority of the maritime population centers and then geographically expands to cover all ports/facilities with mobile enrollment centers. All enrollment centers will be staffed by trained trusted agents who will be subject to a thorough threat assessment. The NPRM allows for pre-enrollment through secure Internet connections and dedicated kiosks.

H. Costs

Comment: NMSAC stated that the fee should be collected at the time of application from the applicant. Any potential employer reimbursements or other business relationships should not be defined in the regulation. Individuals who have already been screened to an equal or higher standard than the TWIC, such as the assessment done for a hazmat endorsement, should not have to pay for duplicate applications, credential issuance, and background records check. TSA should collect only the costs of the program, and the cost for TWIC should be standardized at all enrollment centers.

Response: We agree. The NPRM states that the fee is collected from the applicant at the time of enrollment and does not require any reimbursement arrangements. Also, we propose comparability standards so that agencies with similar checks can apply to TSA for a comparability determination. As for hazmat drivers, the check they must complete to get a hazmat endorsement is the same as the standard for TWIC. Therefore, drivers are not required to complete both checks, but must pay a reduced fee for TWIC enrollment and credential production because it was not included in the hazmat fee or process.

I. Term of Validity

Comment: The TWIC should be valid for a period of five years, unless revoked for cause. This recommendation assumes there is continual check on applicants.

Response: We agree and propose a 5-year period of validity for the TWIC unless revoked for cause. TSA repeats portions of the check throughout the 5-year term.

J. Roll-out Strategy

Comment: NMSAC supported a phased in regional implementation. A timeline and deadline should be identified by TSA, and the final implementation/compliance date

should be consistent across the country and provide sufficient advance lead time to allow stakeholders to prepare. To accommodate U.S. mariners, NMSAC proposed that DHS allow enrollment centers be set up at foreign facilities with a Coast Guard presence.

Response: We agree and section 1572.19 proposes the implementation timeline for applicants to enroll for a TWIC. Regarding oversees enrollment of U.S. mariners, we recognize that is an issue in need of resolution. As credentialed U.S. mariners pose less of a security risk due to the successful completion of security and safety background checks, they have been identified as a population who could potentially be lower on the priority list for receipt of the TWIC. In the meantime, options such as setting up TWIC enrollment stations within existing Coast Guard overseas facilities is being explored.

K. TWIC requirement for access to Sensitive Security Information

Comment: NMSAC recommended that TWIC be used as identification credential alone, and not affect access to SSI.

Response: The statute requires "individuals with access to security sensitive information as determined by the Secretary" to hold a TWIC. We agree that requiring all individuals with access to SSI to also hold a TWIC may be impractical. We have interpreted the language of the statute to allow that only certain individuals who will require access to SSI hold a TWIC, if they have not already been subject to an equivalent check. These individuals are clearly identified by position in the NPRM.

L. Miscellaneous Issues

Comment: NMSAC strongly urges TSA and Coast Guard to gather industry input in the TWIC rulemaking.

Response: In developing the TWIC program, we have benefited from the expertise and assistance of industry and government stakeholders. Our work with the NMSAC has produced several outstanding recommendations and solutions to potential challenges. Additionally, we are planning four public meetings on this NPRM, in order to engage industry and gather comments before a final rule is in place.

Comment: NMSAC urged TSA and Coast Guard to coordinate TWIC with other federal programs to avoid duplication and conflicts. It also urged that Merchant Mariner Licenses and Documents be merged with TWIC to the greatest extent possible to minimize the number of credentials mariners are required to carry.

Response: The Coast Guard National Maritime Center has expressed similar concerns over adding yet another credential to the list of those required for mariners. In a separate rulemaking published in today's Federal Register, the Coast Guard has proposed combining all merchant mariner credentials into a single form, in order to minimize the number of credentials a mariner must carry. That proposal would merge the existing mariner documents, consisting of the License, Merchant Mariner Document, STCW Endorsement, and Certificate of Registry, into one. The TWIC would remain the identification credential and separate from these other credentials, at least for the time being. The consolidated mariner form would document the mariner's professional skills and capabilities and the TWIC would document the mariner's identity.

M. Procedures for Replacement of Lost or Stolen Credentials, and Penalties for Persons who Fraudulently Obtain or Use/Attempt to Use a TWIC.

Comment: NMSAC expressed concerns about the procedures to address lost or stolen credentials, and the penalty for persons who fraudulently obtain or use/attempt to use a TWIC.

Response: We agree that procedures for lost or stolen credentials are essential services. Applicants will be given an 800-number to call in the event they lose the TWIC or it is stolen. The applicant must return to an enrollment center to activate a new TWIC. This will not require a full enrollment process unless the biometric or biographic information has changed since the time of the initial enrollment and the period of validity of the TWIC will be the same as the lost or stolen credential it is replacing. As the NPRM states, applicants who fraudulently obtain or attempt to use a TWIC may be prosecuted criminally and/or through administrative action.

N. On-site TWIC Implementation.

Comment: NMSAC expressed concern about the possibility for delay at points of entry due to implementation of theTWIC program.

Response: During TSA's Prototype, possession of a TWIC ultimately accelerated access for individuals when they were entered into the local access control system. We anticipate similar results when TWIC is fully operational. As proposed, this rule would permit owners/operators to determine the details of the access control system, and so resolving access problems would largely be managed at the facility or vessel. However, we welcome industry feedback and insight on ways that we may be able to improve the proposed requirements without compromising either security or function.

V. Section-by-Section Analysis of United States Coast Guard Proposed Rule

General Introduction

The following discussion highlights the changes being made to the Coast Guard regulations and address some miscellaneous effects that these changes will have on unamended sections of the regulations. The discussion is divided into parts and sections within those parts, which will enable the reader to skip to those regulations that affect him/her. In order to allow for this, some explanations are repeated from part to part (for example, the explanation for proposed amendments to the recordkeeping requirement sections in parts 104, 105, and 106, are identical).

33 CFR Part 101

33 CFR 101.105

Coast Guard proposes amending § 101.105 by adding new definitions for escorting, personal identification number (PIN), recurring unescorted access, secure area, TWIC, TWIC program, and unescorted access. These terms would be introduced by the amendments discussed below, and their definitions are self-explanatory.

33 CFR 101.121

Coast Guard proposes adding § 101.121 to require those organizations that have approved Alternative Security Programs (ASPs) to submit a TWIC Addendum to their ASP. This TWIC Addendum should explain how the TWIC requirements proposed in parts 104, 105, and 106 (as applicable) would be implemented in the ASP. The TWIC Addendum would be submitted to the Coast Guard for approval and, once approved, would be given the same expiration date as the overall ASP. When it is time for the overall ASP to be reapproved, the TWIC Addendum would be incorporated into the overall ASP, resulting in a single document. Any organization not submitting the TWIC Addendum by the given deadline would have their ASP declared invalid.

33 CFR 101.514

Coast Guard proposes adding § 101.514. This new section contains the requirement that all persons requiring unescorted access to secure areas of vessels, facilities, and OCS facilities regulated by parts 104, 105, or 106 of subchapter H possess a TWIC before such access is granted. Federal officials would not be required to use a TWIC, but rather would be required to use their HSPD 12-compliant agency credential. These HSPD 12-compliant, biometrically-enabled credentials will be built according to the same technical standards as the TWIC, ensuring comparable levels of security. Coast Guard has also included a provision allowing for State and local officials to voluntarily obtain a TWIC when their office or duty station falls within, or where they require recurring unescorted access to, a secure area of a vessel, facility, or an OCS facility. Coast Guard would not, at this time, require these officials to obtain a TWIC, but we may revisit this in the future.

Coast Guard also would allow for voluntary compliance with TWIC for those maritime facilities and vessels that would otherwise not be required to comply. Any owner or operator who would like to voluntarily comply with TWIC requirements would first be required to contact their cognizent COTP, who will forward the request, along with the COTP's recommendation, to TSA. Once the Coast Guard and TSA determine that use of the TWIC by the facility or vessel would benefit and improve overall maritime security, the owner/operator would receive authorization to have employees enroll at TSA enrollment centers and establish a TWIC program at their facility. Coast Guard requests that those owner/operators who would like to voluntarily comply under this provision please submit a comment.

33 CFR 101.515

Coast Guard proposes amending § 101.515 to limit its application only to those persons seeking escorted access to a secure area. This amendment would require that anyone, other than law enforcement officers in performance of their official duties, seeking access to a vessel, facility, or OCS facility provide personal identification meeting the standards listed in this section. It also would require that these individuals be escorted at all times in a secure area.

33 CFR Part 103

33 CFR 103.305

Coast Guard proposes amending § 103.305 to require that all Area Maritime Security (AMS) Committee members hold a TWIC or have passed a comparable security background investigation, as determined by the FMSC, with the exception of credentialed Federal, state and local officials. Coast Guard would omit credentialed Federal, state, and local officials from the requirement to hold a TWIC because the majority of these individuals undergo a security threat assessment prior to beginning their job, and because (as explained above) the Federal officials will all be issued HSPD 12-compliant, biometric identification credentials, and it is hoped that states and local entities will follow suit.

33 CFR 103.505 and 103.510

Coast Guard proposes amending §§ 103.505 and 103.510 to require that all AMS plans address biometric access programs within the port, and to require that all AMS plans be updated to reflect this consideration.

33 CFR Part 104

33 CFR 104.105

Coast Guard proposes amending § 104.105 to exempt foreign vessels from the TWIC requirements. Currently foreign vessels entering U.S. ports that carry a valid International Ship and Port Facility (ISPS) certificate are deemed to be in compliance with part 104, except for §§ 104.240, 104.255, 104.292, and 104.295. However, there are a small number of foreign vessels who are not required to comply with the International Convention for Safety of Life at Sea (SOLAS) or with the ISPS Code, and therefore must submit security plans in accordance with this part. Without the proposed language, these vessels would be required to comply with the TWIC provisions. The crew of these vessels would primarily consist of foreign mariners. While not explicitly exempt from the TWIC requirements by the language of 46 U.S.C. 70105, the particular situation of foreign mariners makes it impractical to issue this population TWICs, and it has been determined that it is inappropriate to this rulemaking. Thus, the small number of foreign vessels who would otherwise be required to comply with part 104, as well as all other foreign vessels, have been exempted from complying with the TWIC provisions of this part since none of their crew would hold a TWIC. Nothing in this proposed exemption should affect the existing requirements that owners or operators have procedures in place for allowing seafarers to traverse facilities for the purpose of completing crew changes or taking shore leave.

33 CFR 104.106

Coast Guard proposes adding § 104.106 to provide for passenger access areas on board passenger vessels, ferries, and cruise ships. Implementation of the TWIC credential would have a significant impact on the way that owners and operators make

access control decisions. The proposed rule would introduce the concept of a "secure area," defined as the area over which an owner or operator chooses to exercise access control as set forth in §104.265, essentially making the entire vessel a secure area. In non-passenger vessels, this is not problematic; for those that carry passengers, however, it presents difficulties. Since the law requires that no one be allowed unescorted access to secure areas unless they carry a TWIC, passenger vessels, ferries, and cruise ships would have had to either require passengers to obtain TWICs or ensure that passengers were "escorted" at all times while on the vessel. To avoid either outcome, Coast Guard proposes creating the "passenger access area," which will allow vessel owners/operators to carve out areas within the secure areas aboard their vessels where passengers are free to move about unescorted. These passenger access areas would work in a manner similar to the already existing "public access areas" in part 105.

33 CFR 104.115

In § 104.115, Coast Guard proposes using the same roll-out and implementation model for TWIC as was used for vessel security plans. Vessels would have six (6) months from the date that the final rule is published to submit a TWIC addendum to the Marine Safety Center. They would be required to be operating according to the addendum between twelve (12) and eighteen (18) months following the date that the final rule is published, depending on whether enrollment for the port in which the vessel is operating has been completed.

33 CFR 104.120

The proposed amendment to § 104.120 would require that a copy of the approved TWIC addendum be kept on board the vessel, along with the already approved Vessel

Security Plan (VSP) (already required to be on board). Coast Guard has included provisions for scenarios in which the TWIC addendum has been submitted to the Marine Safety Center (MSC) but not yet approved, and for vessels operating under an approved alternative security program.

33 CFR 104.200, 104.210, 104.215, 104.220, and 104.225

Coast Guard proposes amending these sections to require that all individuals with security duties, including the company security officer (CSO), acquire and maintain a TWIC. Coast Guard requests comment on whether owners/operators should also be required to obtain a TWIC, based on their access to sensitive security information (SSI). Coast Guard also proposes amending these sections to add knowledge requirements and responsibilities pertaining to TWIC to those already assigned to owners/operators, company security officers, vessel security officers, vessel employees with security duties, and all vessel employees. At this time, there are no formal training requirements proposed in order to meet the TWIC knowledge requirements. It is important that owners/operators and those with security duties be familiar with the technologies on the credential that make it resistant to tampering and forgery. Persons who will be examining TWICs at access control points should be familiar enough with its physical appearance such that variations or alterations are easily recognized.

It is important that security personnel at the access points to the vessel be familiar with alternate ways to reliably verify an individual's identity and his or her credential should the individual be unsuccessful using the primary means of verification (e.g., fingerprint match). Personnel who will be required to resolve an individual's failure to electronically verify his or her identity should be familiar with all the possible reasons for

the failure. For example, an individual may not be able to verify his identity against the biometric stored on the credential due to wear on the integrated circuit chip (ICC) itself, problems with the reader, wear on the individual's fingerprints, or because the individual is an imposter. Alternate procedures for addressing failures of an individual to verify his fingerprint against the information stored on the credential should be reasonably designed to discern between a legitimate user and an imposter. All other employees should be familiar with the TWIC topology, as well as the steps to take should their own TWIC become lost or stolen.

The heaviest burden has been placed on the owner/operator, who would be required to ensure that the TWIC program is implemented on board the vessel in accordance with the proposed regulations. This would include a new requirement that the owner/operator ensure that someone on the vessel know who is on the vessel at all times. It would also include a requirement that the owner/operator ensure that computer and access control systems and hardware are secure. The Coast Guard has placed a sample document in its docket (located at the places listed in the ADDRESSES section above) for this NPRM that outlines the proper standard of care to be used to protect these systems and hardware. We request comment on this standard of care, as well as on any associated costs to implement it.

33 CFR 104.235

Coast Guard proposes adding a new record-keeping requirement, mandating that owners/operators maintain records for two years of all persons who are granted access to secure areas of the vessel, including when they disembark the vessel. The requirement does not distinguish between those who were granted unescorted access because they

carried a TWIC and those who were granted escorted access. For those who are granted recurring unescorted access, such as permanently attached crew or other employees, owners/operators would be required to record the span over which the individual's access privileges endured. For individuals who were granted escorted access, the owners/operators would be required to record each date that the individual is escorted, and identify his escort.

33 CFR 104.265

Coast Guard proposes amending this section to require the use of TWIC in the vessel's access control measures. This section would show the greatest changes as a result of TWIC implementation, and reflects a difficult compromise of many competing concerns, including our desire to preserve as much of the performance-based standard as possible so that vessels could tailor implementation to suit their individual operational needs while preserving the security enhancements provided by the TWIC credential.

TWIC provides for implementing graduated security measures by relying upon the three factor authentication process for establishing a person's identity. This process consists of identifying: 1) something the person has - a TWIC credential; 2) something the person knows - a PIN, stored securely on the ICC in the credential; and 3) something the person is - in the case of the TWIC, that will be the individual's fingerprint, which also is stored on the ICC of the credential. By requiring one or all of these factors before allowing access, owners/operators can make increasingly more secure decisions regarding individuals who are requesting to board the vessel.

Currently, most access control decisions are made relying on a "flash pass." Individuals requesting entry are required to show identification that conforms to

§ 101.515 of subchapter H, which currently encompasses a broad spectrum of credentials, including driver's licenses from all 50 states. Many of these credentials are easily forged or altered, and the sheer diversity of appearances hampers security personnel's ability to recognize a forged or altered credential when it is presented.

Even when used as a flash pass, the TWIC provides greater reliability than the existing system because it presents a uniform appearance with embedded features on the face of the credential that make it difficult to forge or alter. When presented with a TWIC, security personnel familiar with its security features are immediately able to notice any absence or destruction of these features.

Nevertheless, our intent was to discourage the use of the TWIC as a flash pass for several reasons. While security personnel can reliably detect changes to the appearance of the credential or missing features, he or she cannot know whether or not the credential has been revoked by TSA, or other competent authority, merely by examining the surface of the credential. Furthermore, comparing the individual to the photo on the credential requires focused examination that is likely to suffer when security personnel are distracted or during particularly busy periods. This is the time that an unauthorized individual is most likely to attempt entry, and is most likely to breach a system that relies solely on the flash pass system. Finally, allowing owners/operators to rely solely on the flash pass system is unreasonable in light of the additional cost of the credential, and the available security enhancements that the increased cost represents.

Thus, Coast Guard proposes to require owners/operators to use at least one of the technical enhancements on the credential to electronically verify a person's identity and

also requires verification that the credential remains valid, and has not been altered or counterfeited.

Implementation of the TWIC program will require that the owner/operator use different processes for identifying persons, depending on whether or not the individual is requesting unescorted access. If the individual is requesting, or will require, unescorted access as part of his or her job responsibilities, the individual must have and maintain a TWIC.

On an owner/operator's first encounter with an individual seeking or requiring unescorted access to the vessel, we would require that all of TWIC's security features be used to verify both the individual's claimed identity and that the credential remained valid. Thus, when presented with an individual's TWIC for the first time, an owner or operator would be required to electronically verify that the individual's fingerprint matches the data stored on the ICC, and that the individual can correctly enter the PIN that is also stored on the ICC. Both of these processes will require that the individual have the TWIC in his/her possession, thus satisfying all three factors of the authentication process. In addition, the owner or operator would have to confirm that the TWIC remains valid. In order to know that the TWIC has not been revoked, some regular contact with TSA will be necessary. Coast Guard has not specified how this contact should be made so as to provide as much flexibility as possible.

These steps performed together will detect to the highest degree of certainty whether the individual is the rightful bearer of the TWIC he or she holds, and whether or not it was duly issued and remains valid. After the initial encounter, there is as much flexibility as possible for the owner/operator so that the TWIC would provide a valuable

security enhancement without unnecessarily burdening daily operations. Coast Guard recognized that, particularly for smaller vessels such as towing vessels, the value by the daily validation of an individual's personal identity is less than for facilities, which generally interact with greater numbers of vendors, visitors, and facility employees. We assumed that the crew of most vessels, excluding cruise ships, would be a relatively small number of people who would quickly become familiar enough with one another so as to be able to readily identify fellow crew members and notice strangers. Thus, there is more emphasis on ensuring that the credential remains valid. Accordingly, Coast Guard has identified specific intervals, according to the Maritime Security (MARSEC) level, when a vessel owner/operator must routinely check that the credential remains valid.

As a result of this desire to provide flexibility, we propose the concept of "recurring unescorted access," which is intended to allow an individual to enter on a continual basis, without repeating the personal identity verification piece. The decision to grant recurring access privileges should be based on two considerations: 1) the relationship of the individual to the vessel, or how well "known" he or she is; and 2) the individual's need to have frequent and unimpeded access to the vessel.

No vessel is required to grant any individual recurring unescorted access; it is intended as a tool by which owners/operators can allow persons who are well known to them to move in and out of secure areas on a repetitive basis without having to electronically verify the individual's identity each time. The credential verification requirement would remain, and owners/operators would be responsible to check the validity of the TWIC belonging to any person to whom is granted recurring unescorted access according to the identified specific interval, based on the MARSEC level.

Frequent vendors and other visitors, such as union and seafarer representatives, could seek and, at the owner/operator's discretion, be granted recurring unescorted access. If granted, it would allow these individuals, identified by the vessel security officer, or other qualified personnel, to be entered onto the vessel's rolls of TWIC holders whose TWIC must be checked on a regular basis to ensure it remains unrevoked by TSA.

The infrequent visitor or vendor who bears a TWIC and seeks unescorted access, would be required to electronically verify his or her identity by matching the biometric information stored on the ICC. The credential's validity would also have to be verified to ensure that it has not been revoked since issuance by TSA. Coast Guard acknowledges that maintaining this connectivity with TSA will be a challenge for vessel owners and operators. However, TSA has indicated that it will be able to maintain an updated list of all invalid credentials which can be downloaded over a secure connection with the TSA Web site, and vessel owners/operators would be able to verify the validity of credentials from infrequent visitors against this list. Furthermore, Coast Guard has assumed that vessels which could not establish access to TSA via a secure Web site from time to time could obtain updated versions of the list from its agent or home office.

Persons presenting for entry who do not hold a TWIC would still be required to show an acceptable form of identification, as set forth in § 101.515 and 104.265(e)(3), and would be required to be escorted if they are granted access to secure areas. Owners/operators are not required by the proposed changes to use the TWIC as their primary badging system. As much as practical, Coast Guard has retained the performance-based standards from the existing regulations that allows owners/operators to establish identification systems that best suits their individual operational needs. If,

however, owners/operators choose to rely solely on the TWIC as their badging system, the system should include a means for identifying non-TWIC holders. If owners/operators choose to use a separate badging system, it must be coordinated with the TWIC requirements in this part such that notification to the owner/operator of changes in the individual's TWIC status are also reflected in the separate badging system.

Other existing regulatory requirements that we thought were important to preserve related to coordinating access control measures and the TWIC implementation with facilities whenever possible, particularly as that would facilitate the ready access of frequent vendors, and union and seafarer representatives to the vessel, as appropriate. Coast Guard anticipates that these individuals will also obtain a TWIC. Any coordination must be outlined in the TWIC addendum.

In keeping with the longstanding tradition that seafarers keep their mariner credentials and other important documents on the bridge, or stored in a secure place, this rule does not propose that vessel crew be required to display or maintain their TWIC on their person at all times. Instead, anyone granted unescorted access to the secure areas of the vessel under this proposed rule is expected to produce his or her TWIC for inspection if so required by a competent authority. Thus, persons assigned to the vessel can keep the credential stored securely on the vessel with their other important documents. However, mariners will have to take the TWIC with them when they leave the vessel in order to gain unescorted access through the facility.

Owners/operators are required to devise backup processes for making access control decisions when any part of the TWIC system fails, with particular attention paid to not creating greater vulnerabilities that can be leveraged by a failure of the system due

to deliberate efforts. Of particular concern is the occasion when an individual may not be able to match his or her biometric against the information stored on the ICC. While this could mean the person is not who he says he is, it is also possible that wear and tear on the reader, the ICC, or the person's fingerprint itself have caused the failure. In resolving these kinds of failures, security personnel should be well informed as to other reliable means of verifying identity, such as comparing the image of the individual that is electronically stored on the ICC to the person him or herself, or by having other authorized personnel vouch for his identity.

In keeping with the graduated scheme of the MTSA regulations, this rule proposes requiring increased use of TWIC security features at higher MARSEC levels. At MARSEC level 1, the owner/operator would be required to ensure that the validity of TWIC credentials is verified against the latest information available from TSA on a weekly basis. At MARSEC level 2, the owner/operator would be required to ensure that the validity of TWIC credentials is verified against the latest information available from TSA on a daily basis. At MARSEC level 3, all personnel seeking unescorted access would be required to verify their identity biometrically and using their PIN at each entry to a secure area of the vessel.

The requirements at each MARSEC level are laid out in the table that follows.

	VESSELS		FACILITIES	OCS FACILITIES	U.S. FLAGGED CRUISE SHIPS
	Recurring Unescorted Access	Non-Recurring Unescorted Access			
MARSEC 1	Facial recognition minimum each entry; card	1 to 1 biometric match at each entry; card	1 to 1 biometric match at each entry; card validity	1 to 1 biometric match at each entry;	1 to 1 biometric match at each entry; card validity

	validity checked weekly with information ≤ 1 week old	validity checked at each entry with information ≤ 1 week old	checked at each entry with information ≤ 1 week old	card validity checked at each entry with information ≤ 1 week old; recheck those continuously aboard weekly with most current information available from TSA	checked at each entry with most current information available from TSA
MARSEC 2	Facial recognition minimum each entry; card validity checked daily with most current information available from TSA	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those continuously aboard daily with most current information available from TSA	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with most current information available from TSA
MARSEC 3	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old		1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those aboard continuously daily	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with most current information available from TSA

33 CFR 104.290

Coast Guard proposes amending this section to require owners/operators to have the records of persons who have been granted access to the vessel (See, § 104.235, discussed above) available after a security incident.

33 CFR 104.295

Coast Guard proposes amending § 104.295 to impose higher burdens on U.S. cruise ships. The same assumptions regarding crew size and connectivity (discussed in the proposed changes to §104.265 above) do not apply to these large, sophisticated vessels whose potential to be the impetus of a transportation security incident (TSI) is much greater than other vessels. As a result, TWIC requirements more closely resemble those for facilities. Coast Guard proposes requiring that an individual's identity be checked against their TWIC at each entry to the vessel, and that the validity of the TWIC be verified with TSA at a higher rate than for other vessels.

33 CFR 104.405

Coast Guard proposes amending this section to require that when each vessel security plan is reviewed and resubmitted for approval upon its 5 year anniversary date, it incorporates the TWIC Addendum into all appropriate sections of the VSP. Most of these changes should be reflected in the plan's section on access control.

New Subpart E (33 CFR 104.500 – 104.510)

Proposed § 104.500-104.510 are new and are intended to be temporary measures that will be phased out as existing plans are renewed according to their expiration date. Rather than require owners/operators to resubmit their entire plan with the TWIC measures incorporated within, Coast Guard proposes requiring a temporary TWIC addendum to be submitted. The addendum should be drafted in conjunction with the

existing plan, reflecting all modifications that the TWIC rules require. Once approved, it should be attached to and maintained as part of the entire plan, and will be given the same expiration date as the existing plan. Upon expiration, the TWIC addendum should be seamlessly incorporated into the full plan when it is renewed in accordance with the regulations in place at the time of renewal. Owners/operators may opt to resubmit their entire plan, with a list of sections amended, as their TWIC Addendum, but once approved it will carry the same expiration date as it had prior to amendment. Owners/operators are encouraged to submit the addendum via Homeport (http://homeport.uscg.mil).

33 CFR Part 105

33 CFR 105.115

In § 105.115, Coast Guard proposes using the same roll-out and implementation model for TWIC as was used for MTSA security plans. Facilities would have six (6) months from the date that the final rule is effective to submit a TWIC addendum to their cognizant Captain of the Port (COTP) and would be required to be operating according to the addendum between twelve (12) and eighteen (18) months following the effective date, depending on whether enrollment has been completed at the port where the facility is located.

33 CFR 105.120

In the proposed amendment to § 105.120, Coast Guard would require that the facility keep a copy of the approved TWIC addendum on-site, along with the already approved facility security plan (FSP) (already required to be on site). Coast Guard has included provisions for scenarios in which the TWIC addendum has been submitted to

the COTP but not yet approved, and for facilities operating under an approved alternative security program.

33 CFR 105.200, 105.205, 105.210, and 105.215

Coast Guard proposes amending these sections to require that all individuals with security duties acquire and maintain a TWIC. Coast Guard requests comment on whether owners/operators should also be required to obtain a TWIC, based on their access to sensitive security information (SSI). Coast Guard also proposes adding knowledge requirements and responsibilities pertaining to TWIC to those already assigned to owners/operators, facility security officers, facility employees with security duties, and all facility employees. There are no formal training requirements in order to meet the TWIC knowledge requirements proposed at this time. It is important that owners/operators and those with security duties be familiar with the technologies on the credential, particularly the imbedded features that make the credential resistant to tampering and forgery. Persons who will be examining TWICs at access control points should be familiar enough with its physical appearance such that variations or alterations are easily recognized.

It is important that security personnel at the access points to the facility be familiar with alternate ways to reliably verify an individual's identity and his or her credential should the individual be unsuccessful using the primary means of verification (e.g., fingerprint match). For example, an individual may not be able to verify his identity against the biometric stored on the credential due to wear on the ICC itself, problems with the reader, wear on the individual's fingerprints, or because the individual is an imposter. Alternate procedures for addressing failures of an individual to verify his

fingerprint against the information stored on the credential should be reasonably designed to discern between a legitimate user and an imposter. All other employees should be familiar with the TWIC topology, as well as the steps to take should their own TWIC become lost or stolen.

The heaviest burden has been placed on the owner/operator, who would be required to ensure that the TWIC program is implemented on board the facility in accordance with the proposed regulations. This would include a new requirement that the owner/operator ensure that someone on the facility know who is on the facility at all times. It would also include a requirement that the owner/operator ensure that computer and access control systems and hardware are secure. The Coast Guard has placed a sample document in its docket (located at the places listed in the ADDRESSES section above) for this NPRM that outlines the proper standard of care to be used to protect these systems and hardware. We request comment on this standard of care, as well as on any associated costs to implement it.

33 CFR 105.225

Coast Guard proposes adding a new record-keeping requirement, mandating that owners/operators maintain records for two years of all persons who are granted access to the facility. The requirement does not distinguish between those who were granted unescorted access because they carried a TWIC and those who were granted escorted access. For individuals who were granted escorted access, the owners/operators would be required to record each date that the individual is escorted, and identify his escort.

33 CFR 105.255

Coast Guard proposes amending this section to require the use of TWIC in the facility's access control measures. This section would show the greatest changes as a result of TWIC implementation, and reflects a difficult compromise of many competing concerns, including our desire to preserve as much of the performance-based standard as possible so that facilities could tailor implementation to suit their individual operational needs while preserving the security enhancements provided by the TWIC credential. TWIC provides graduated increases in security by relying upon the three factor authentication process for establishing a person's identity. This process consists of identifying: 1) something the person has - a TWIC credential; 2) something the person knows - a Personal Identification Number (PIN), stored on the integrated circuit chip (ICC) in the credential; and 3) something the person is - in the case of the TWIC, it will be the individual's fingerprint, which is also stored on the ICC of the credential. By requiring one or all of these factors before allowing access, owners/operators can make increasingly more secure decisions regarding individuals who are requesting to enter the facility.

Currently, most access control decisions are made relying on a "flash pass." Individuals requesting entry are required to show identification that conforms to § 101.515 of subchapter H, which currently encompasses a broad spectrum of credentials, including driver's licenses from all 50 states. Many of these credentials are easily forged or altered, and the sheer diversity of appearances hampers security personnel's ability to recognize a forged or altered credential when it is presented.

Even when used as a flash pass, the TWIC provides greater reliability than the existing system because it presents a uniform appearance with embedded features on the

face of the credential that make it difficult to forge or alter. When presented with a TWIC, security personnel familiar with its security features are immediately able to notice any absence or destruction of these features.

Nevertheless, our intent was to discourage the use of the TWIC as a flash pass for several reasons. While security personnel can reliably detect changes to the appearance of the credential or missing features, he or she cannot know whether or not the credential has been revoked by TSA, or other competent authority, merely by examining the surface of the credential. Furthermore, comparing the individual to the photo on the credential requires focused examination that is likely to suffer when security personnel are distracted or during particularly busy periods. This is the time that an unauthorized individual is most likely to attempt entry, and is most likely to breach a system that relies solely on the flash pass system. Finally, allowing owners/operators to rely solely on the flash pass system is unreasonable in light of the additional cost of the credential, and the available security enhancements that the increased cost represents.

Thus, Coast Guard proposes to require owners/operators to use at least one of the technical enhancements on the credential to electronically verify a person's identity and also requires verification that the credential remains valid, and has not been altered or counterfeited.

Implementation of TWIC will require that the owner/operator use different processes for identifying persons depending on whether or not the individual is requesting unescorted access. If the individual is requesting unescorted access, or will require unescorted access as part of his or her job responsibilities, the individual must have and maintain a TWIC.

Individuals requesting unescorted access to secure areas of the facility must present a valid TWIC prior to entry and electronically verify his or her identity by matching his or her biometric against the information stored on the credential.

In addition, the owner or operator would have to confirm that the TWIC remains valid. In order to know that the TWIC has not been revoked, some regular contact with TSA will be necessary. (See, discussion of "using TWIC in an access control system" above.) No particular method has been prescribed for contacting TSA to verify the validity of credentials so as to provide as much flexibility to owners/operators as possible.

Persons presenting for entry who do not hold a TWIC would still be required to show an acceptable form of identification, as set forth in §§ 101.515 and 104.265(e)(3), and will be required to be escorted if they are granted access to secure areas. Owners/operators are not required by the proposed changes to use the TWIC as their primary badging system. As much as practical, the rule proposed to retain the performance-based standards from the existing rule that allows owners/operators to establish identification systems that best suit their individual operational needs. If, however, owners/operators choose to rely solely on the TWIC as their badging system, the system should include a means for identifying non-TWIC holders. If owners/operators choose to use a separate badging system, it must be coordinated with the TWIC requirements in this part.

Other provisions that are important to preserve are related to coordinating access control measures and the TWIC implementation with vessels whenever possible,

particularly as that would facilitate the ready access of frequent vendors, and union and seafarer representatives to the vessel and crew as appropriate.

Facility personnel are required to have their TWIC readily available for inspection if so required by a competent authority.

Coast Guard proposes that owners/operators be required to devise backup processes for making access control decisions should any part of the TWIC system fail, with particular attention paid to not creating greater vulnerabilities that can be leveraged by deliberately causing a failure of the system. Of particular concern is the occasion when an individual may not be able to match his or her biometric against the information stored on the ICC. While this could mean the person is not who he says he is, it is also possible that wear and tear on the reader, the ICC, or the person's fingerprint itself have caused the failure. In resolving these kinds of failures, security personnel should be well informed as to other reliable means of verifying identity, such as comparing the image of the individual that is electronically stored on the ICC to the person him or herself, or by having other authorized personnel vouch for his identity.

In keeping with the graduated scheme of the MTSA regulations, Coast Guard proposes requiring increased use of the TWIC at higher MARSEC levels. At MARSEC level 1, the owner/operator would be required to ensure the validity of the TWIC credentials is verified against the latest information available from TSA on a weekly basis. At MARSEC level 2, the owner/operator would be required to ensure that the validity of TWIC credentials is verified against the latest information available from TSA on a daily basis, as well as ensure all TWIC-enabled access gates are manned. At

MARSEC level 3, Coast Guard would require verification of an individual's PIN at each entry to the secure area.

The requirements at each MARSEC level are laid out in the table that follows.

	VESSELS		FACILITIES	OCS FACILITIES	U.S. FLAGGED CRUISE SHIPS
	Recurring Unescorted Access	Non-Recurring Unescorted Access			
MARSEC 1	Facial recognition minimum each entry; card validity checked weekly with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old; recheck those continuously aboard weekly with most current information available from TSA	1 to 1 biometric match at each entry; card validity checked at each entry with most current information available from TSA
MARSEC 2	Facial recognition minimum each entry; card validity checked daily with most current information available from TSA	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those continuously aboard daily with most current information available from TSA	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with most current information available from TSA
MARSEC 3	1 to 1 biometric match + PIN at each entry; card		1 to 1 biometric	1 to 1 biometric	1 to 1 biometric match + PIN at

	validity checked at each entry with information ≤ 1 day old	match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old	match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those aboard continuously daily	each entry; card validity checked at each entry with most current information available from TSA

33 CFR 105.280

This section would be amended to require owners/operators to have the records of persons who have been granted access to the facility (See § 105.225, discussed above) available after a security incident.

33 CFR 105.285

This section would be amended to clarify that passengers must be escorted within secure and restricted areas of the facility.

33 CFR 105.290

This section would be amended to clarify which activities must be done within the facility's secure area, to clarify the identifications to be checked before granting individuals entry to the facility, and to clarify that passengers must be escorted within secure and restricted areas of the facility.

33 CFR 105.295

Coast Guard proposes making a change to clarify that persons not holding TWICs must be escorted within Certain Dangerous Cargo (CDC) facilities. Coast Guard asks for comment as to whether there should be more stringent TWIC program requirements at these facilities, and what those requirements should be.

33 CFR 105.296

Coast Guard proposes amending § 105.296 to require that owners/operators of barge fleeting facilities take responsibility for ensuring that anyone seeking unescorted access to barges within the fleeting facility hold a TWIC.

33 CFR 105.405

This section would be amended to require that when each facility security plan is reviewed and resubmitted for approval upon its 5-year anniversary date, it incorporate the TWIC Addendum into all appropriate sections of the FSP. Most of these changes should be reflected in the plan's section on access control.

New Subpart E (33 CFR 105.500 – 105.510)

Proposed §§ 105.500-105.510 are new and are intended to be temporary measures that will be phased out as existing plans are renewed according to the existing plan's expiration date. Rather than require owners/operators to resubmit their entire plan with the TWIC measures incorporated within, we propose requiring a temporary TWIC addendum to be submitted. The addendum should be drafted in conjunction with the existing plan, reflecting all modifications that the TWIC rules require. Once approved, it should be attached to and maintained as part of the entire plan, and will be given the same expiration date as the existing plan. Upon expiration, the TWIC addendum should be seamlessly incorporated into the plan when it is renewed in accordance with the regulations in place at the time of renewal. Owners/operators may opt to resubmit their entire plan, with a list of sections amended, as their TWIC Addendum, but once approved it will carry the same expiration date as it had prior to amendment. Owners/operators are encouraged to submit the addendum via Homeport (http://homeport.uscg.mil).

33 CFR Part 106

33 CFR 106.110

In § 106.110, Coast Guard proposes using the same roll-out and implementation model for TWIC as was used for MTSA security plans. OCS facilities would have six (6) months from the date that the final rule is published to submit a TWIC addendum to their cognizant District Commander and would be required to be operating according to the addendum between twelve (12) and eighteen (18) months following the publication date, depending on whether enrollment has been completed at the port where the facility is located.

33 CFR 106.115

The proposed amendment to § 106.115 would require that the OCS facility keep a copy of the approved TWIC addendum on site, along with the already approved OCS FSP (already required to be on site). This proposed rule includes provisions for scenarios in which the TWIC addendum has been submitted to the District Commander but not yet approved, and for OCS facilities operating under an approved alternative security program.

33 CFR 106.200, 106.205, 106.210, 106.215, and 106.220

These sections would be amended to require that all individuals with security duties, including the CSO, acquire and maintain a TWIC. Coast Guard requests comment on whether owners/operators should also be required to obtain a TWIC, based on their access to sensitive security information (SSI). This proposal would also amend these sections to add knowledge requirements and responsibilities pertaining to TWIC to those already assigned to owners/operators, company security officers, OCS facility

security officers, OCS facility employees with security duties, and all OCS facility employees. There are no formal training requirements in order to meet the TWIC knowledge requirements at this time. It is important that owners/operators and those with security duties be familiar with the technologies on the credential, particularly the imbedded features that make the credential resistant to tampering and forgery. Persons who will be examining TWICs at access control points should be familiar enough with its physical appearance such that variations or alterations are easily recognized.

It is important that security personnel at the access points to the OCS facility be familiar with alternate ways to reliably verify an individual's identity and his or her credential should the individual be unsuccessful using the primary means of verification (e.g., fingerprint match). Personnel who will be required to resolve an individual's failure to electronically verify his or her identity should be familiar with all the possible reasons for the failure. For example, an individual may not be able to verify his identity against the biometric stored on the credential due to wear on the ICC itself, problems with the reader, wear on the individual's fingerprints, or because the individual is an imposter. Alternate procedures for addressing failures of an individual to verify his fingerprint against the information stored on the credential should be reasonably designed to discern between a legitimate user and an imposter. All other employees should be familiar with the TWIC topology, as well as the steps to take should their own TWIC become lost or stolen.

The heaviest burden has been placed on the owner/operator, who would be required to ensure that the TWIC program is implemented on board the OCS facility in accordance with the proposed regulations. This would include a new requirement that

the owner/operator ensure that someone on the OCS facility know who is on the OCS facility at all times. It would also include a requirement that the owner/operator ensure that computer and access control systems and hardware are secure. The Coast Guard has placed a sample document in its docket (located at the places listed in the ADDRESSES section above) for this NPRM that outlines the proper standard of care to be used to protect these systems and hardware. We request comment on this standard of care, as well as on any associated costs to implement it.

33 CFR 106.230

Coast Guard proposes adding a new record-keeping requirement, mandating that owners/operators maintain records for two years of all persons who are granted access to the OCS facility. The requirement does not distinguish between those who were granted unescorted access because they carried a TWIC and those who were granted escorted access.

33 CFR 106.260

Coast Guard proposes amending this section to require the use of TWIC in the OCS facility's access control measures. This section would show the greatest changes as a result of TWIC implementation, and reflects a difficult compromise of many competing concerns, including our desire to preserve as much of the performance based standard as possible so that OCS facilities could tailor implementation to suit their individual operational needs while preserving the security enhancements provided by the TWIC credential.

TWIC provides for implementing graduated security measures by relying upon the three factor identification process for establishing a person's identity. This process

consists of identifying 1) something the person has - a TWIC credential; 2) something the person knows - a Personal Identification Number (PIN), stored on the integrated circuit chip (ICC) in the credential; and 3) something the person is - in the case of the TWIC, it will be the individual's fingerprint, which is also stored on the ICC of the credential. By requiring one or all of these factors before allowing access, owners/operators can make increasingly more secure decisions regarding individuals who are requesting access to the OCS facility.

Currently, most access control decisions are made relying on a "flash pass." Individuals requesting entry are required to show identification that conforms to § 101.515 of subchapter H, which currently encompasses a broad spectrum of credentials, including driver's licenses from all 50 states. Many of these credentials are easily forged or altered, and the sheer diversity of appearances hampers security personnel's ability to recognize a forged or altered credential when it is presented.

Even when used as a flash pass, the TWIC provides greater reliability than the existing system because it presents a uniform appearance with embedded features on the face of the credential that make it difficult to forge or alter. When presented with a TWIC, security personnel familiar with its security features are immediately able to notice any absence or destruction of these features.

Nevertheless, our intent was to discourage the use of the TWIC as a flash pass for several reasons. While security personnel can reliably detect changes to the appearance of the credential or missing features, he or she cannot know whether or not the credential has been revoked by TSA, or other competent authority, merely by examining the surface of the credential. Furthermore, comparing the individual to the photo on the credential

requires focused examination that is likely to suffer when security personnel are distracted or during particularly busy periods. This is the time that an unauthorized individual is most likely to attempt entry, and is most likely to breach a system that relies solely on the flash pass system. Finally, allowing owners/operators to rely solely on the flash pass system is unreasonable in light of the additional cost of the credential, and the available security enhancements that the increased cost represents.

Thus, Coast Guard proposes to require owners/operators to use at least one of the technical enhancements on the credential to electronically verify a person's identity and also requires verification that the credential remains valid, and has not been altered or counterfeited.

Implementation of TWIC will require that the owner/operator use different processes for identifying persons depending on whether or not the individual is requesting unescorted access. If the individual is requesting unescorted access, or will require it as part of their job responsibilities, the individual must have and maintain a TWIC.

For OCS facilities, Coast Guard proposes requiring uniformly that all of TWIC's security features be used to verify both the individual's claimed identity and that the credential remains valid each time an individual seeks unescorted access to the OCS facility. Thus, an owner/operator must ensure some means for completing an electronic verification that the individual's fingerprint is matched to the data stored on the ICC each time an individual seeks unescorted access to the OCS facility. This process will require that the individual have the TWIC in his/her possession, thus satisfying all three factors of the three factor authentication process.

In addition, the owner/operator will have to confirm that the TWIC remains valid. In order to know that the TWIC has not been revoked, some regular contact with TSA is required. The rule would not specify, however, how this contact shall be made, so as to leave as many options open as possible. (See discussion of "using TWIC in an access control system" above.) These steps performed together will detect to the highest degree of certainty whether the individual is the rightful bearer of the TWIC he or she holds, and whether or not it was duly issued and remains valid.

Persons presenting for entry who do not hold a TWIC would still be required to show an acceptable form of identification, as set forth in §§ 101.515 and 106.260(d), and would be required to be escorted if they are granted access to secure areas. Owners/operators are not required by the proposed changes to use the TWIC as their primary badging system. As much as practical, the rule proposes to retain the performance-based standards from the existing rule that allows owners/operators to establish identification systems that best suit their individual operational needs. If, however, owners/operators choose to rely solely on the TWIC as their badging system, the system should include a means for identifying non-TWIC holders. If owners and operators choose to use a separate badging system, it must be coordinated with the TWIC requirements in this part.

Other provisions that we thought were important to preserve related to coordinating access control measures and the TWIC implementation with vessels whenever possible, particularly as that would facilitate the movement of OCS facility employees using offshore supply vessels to gain access to the OCS facility. Any coordination must be outlined in the TWIC addendum.

Owners/operators are required to devise backup processes for making access control decisions when any part of the TWIC system fails, with particular attention paid to not creating greater vulnerabilities that can be leveraged by deliberately causing a failure of the system. Of particular concern is the occasion when an individual may not be able to match his or her biometric against the information stored on the ICC. While this could mean the person is not who he says he is, it is also possible that wear and tear on the reader, the ICC, or the person's fingerprint itself have caused the failure. In resolving these kinds of failures, security personnel should be well informed as to other reliable means of verifying identity, such as comparing the image of the individual that is electronically stored on the ICC to the person him or herself, or by having other authorized personnel vouch for his identity.

In keeping with the graduated scheme of the MTSA regulations, this NPRM proposes requiring increased use of the TWIC at higher MARSEC levels. At MARSEC level 1, the owner/operator would be required to ensure that the validity of TWIC credentials is verified against the latest information available from TSA on a weekly basis. At MARSEC level 2, the owner/operator would be required to ensure that the validity of TWIC credentials is verified against the latest information available from TSA on a daily basis. At MARSEC level 3, Coast Guard would require verification of an individual's PIN at each entry to the secure area.

The requirements at each MARSEC level are laid out in the table that follows.

	VESSELS		FACILITIES	OCS FACILITIES	U.S. FLAGGED CRUISE SHIPS
	Recurring Unescorted Access	Non-Recurring Unescorted Access			

MARSEC 1	Facial recognition minimum each entry; card validity checked weekly with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 week old; recheck those continuously aboard weekly with most current information available from TSA	1 to 1 biometric match at each entry; card validity checked at each entry with most current information available from TSA
MARSEC 2	Facial recognition minimum each entry; card validity checked daily with most current information available from TSA	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those continuously aboard daily with most current information available from TSA	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with most current information available from TSA
MARSEC 3	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old		1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with information ≤ 1 day old; recheck those aboard continuously daily	1 to 1 biometric match + PIN at each entry; card validity checked at each entry with most current information available from TSA

33 CFR 106.280

This section would be amended to require owners/operators to have the records of persons who have been granted access to the OCS facility (See § 106.230, discussed above) available after a security incident.

33 CFR 106.405

This section would be amended to require that when each OCS facility security plan (FSP) is reviewed and resubmitted for approval upon its 5-year anniversary date, it must incorporate the TWIC Addendum into all appropriate sections of the OCS FSP. Most of these changes should be reflected in the plan's section on access control.

New Subpart E (33 CFR 106.500 – 106.510)

Proposed §§ 106.500-106.510 are new and are intended to be temporary measures that will be phased out as existing plans are renewed according to the existing plan's expiration date. Rather than require owners/operators to resubmit their entire plan with the TWIC measures incorporated within, the rule would require a temporary TWIC addendum to be submitted. The addendum should be drafted in conjunction with the existing plan, reflecting all modifications that the TWIC rules require. Once approved, it should be attached to and maintained as part of the entire plan, and will be given the same expiration date as the existing plan. Upon expiration, the TWIC addendum should be seamlessly incorporated into the plan when it is renewed in accordance with the regulations in place at the time of renewal. Owners/operators may opt to resubmit their entire plan, with a list of sections amended, as their TWIC Addendum, but once approved it will carry the same expiration date as it had prior to amendment. Owners/operators are encouraged to submit the addendum via Homeport (http://homeport.uscg.mil).

Miscellaneous Items.

The proposed changes outlined above would affect other sections within 33 CFR subchapter H, even though these sections would not be changed. Some of the greatest impacts are summarized below:

33 CFR 101.305

There are no proposed amendments to this section, but certain incidents involving TWICs would need to be reported as either a suspicious activity or breach of security. For example, under certain circumstances an individual's attempt to gain entry using an invalid TWIC (one that has been revoked or one that is counterfeit) may qualify as suspicious activity, even if that individual was denied access. Circumstance that trigger the reporting requirement in 101.305(a), are highly fact-specific and difficult to define comprehensively, but the general language found within that section ("activities that may result in a transportation security incident") is a good guide.

If an owner/operator, or any other individual holding a TWIC, knows of a reason that an individual who holds a TWIC should have that TWIC revoked, the owner/operator should treat this as suspicious activity and report it as required in 101.305(a). The owner/operator may also deny the TWIC-holder access in this situation. Additionally, finding an individual who does not have a valid TWIC within a secure area would qualify as a breach of security, and should be reported as such pursuant to 101.305(b).

33 CFR 101.400

TSA, as the DHS entity responsible for conducting security threat assessments and issuing credentials under this rule, will have principal enforcement authority in

regard to an individual's TWIC status for the misuse of a TWIC, including forgery, counterfeiting, alteration or use of a TWIC by an unauthorized individual. The Coast Guard will work with TSA where abuses of the TWIC program are identified in the maritime sector. In addition, individuals who try to enter a facility or vessel using a stolen, forged, counterfeit, altered or otherwise unauthorized TWIC, and who are detected and turned away by the facility, may be subject to Coast Guard enforcement actions under 33 CFR 101.415 or other applicable Coast Guard authority, including, but not limited to, civil or criminal penalties.

An owner/operator is required to deny unescorted access to an individual who attempts to access a facility with a TWIC that has been revoked by TSA. Coast Guard is not asking owners/operators to take any additional steps, beyond current requirements, with respect to individuals who attempt unauthorized access to a facility. In such circumstances (e.g., where an individual presents for entry at a facility with a TWIC that has been revoked by TSA or with a TWIC which the owner/operator has reason to believe is invalid due to forgery, adulteration, counterfeiting or possession by an unauthorized individual), however, the owner/operator is required to immediately report the matter to the Coast Guard and/or local law enforcement as required under 101.305.

33 CFR 104.130, 105.130, and 106.125

There are no proposed amendments to these sections. However, note that owners/operators of vessels, facilities and OCS facilities, regulated under parts 104, 105, or 106, respectively, may use the above-cited provisions to apply for waivers from the TWIC requirements. They also may suggest equivalents, under § 101.130. These requests should be made in accordance with the relevant provisions of parts 104, 105, or

106. The Coast Guard, however, will not be responsible for making determinations of requests for waivers from individuals required to obtain a TWIC. TSA is the only agency that may waive the requirement that an individual pass a security threat assessment. No one will be waived from the requirement to actually obtain a TWIC.

33 CFR Subpart C, Parts 104, 105, and 106

When it is time for a vessel, facility, or OCS facility to redo a security assessment, in concert with an update to a security plan, consideration of TWIC implementation must be part of the assessment. The TWIC program implemented by the vessel, facility, or OCS facility becomes part of the baseline security analyzed by the assessment.

46 CFR Parts 10, 12, and 15

In order to implement the MTSA mandate that all credentialed merchant mariners hold a TWIC, the Coast Guard is proposing to amend parts 10, 12, and 15 of title 46 to the CFR to require that any individual holding or working under an MMD or a license also hold a TWIC. Coast Guard, in a separate rulemaking published in today's issue of the Federal Register, is proposing to consolidate merchant mariner credentials to minimize duplicate or redundant identification or background check requirements.

VI. Section-by-Section Analysis of TSA Proposed Rule

TSA proposes to amend and redesignate its existing hazmat regulations to apply those processes to a person who is eligible to obtain a TWIC. TSA does not reiterate substantive analyses of the hazmat provisions below if the standard is not changing, but instead directs the public to the section-by-section analysis of those sections contained in the interim final rule implementing the hazmat regulations at 69 FR 68720. Where

standards that formerly applied only to HME applicants now apply to TWIC applicants, however, TSA provides substantive analyses below for the convenience of potential TWIC applicants.

The following is a discussion of the proposed changes to sections in title 49 of the CFR.

49 CFR Part 1515 Appeal and Waiver Procedures for Security Threat Assessments for Individuals.

49 CFR 1515.1 Scope.

TSA is proposing to redesignate §§ 49 CFR 1572.141 and 143 as new part 1515, Appeal and Waiver Procedures for Land and Maritime Workers to Subchapter A—Administrative and Procedural Rules. TSA developed the appeal and waiver procedures in part 1572 that currently apply to commercial drivers applying for an HME for additional transportation workers who may be subject to the security threat assessment requirement. These are the procedures TSA proposes to apply to TWIC applicants. In addition, TSA may use these procedures for other security threat assessments. For instance, TSA published a proposed rule on air cargo security that included security threat assessment requirements for certain individuals and an appeal procedure that is used currently for HME applicants. 69 FR 65258 (November 10, 2004). It makes more sense, organizationally, to place the appeal rules in a general section of the regulations.

The scope section states that the standards in part 1515 apply to an applicant who undergoes a security threat assessment and wishes to appeal an adverse decision or file a waiver request.

49 CFR 1515.3 Terms used in this part.

This section lists definitions of terms that apply specifically to the appeal and waiver process. The term "applicant" is amended to include individuals applying for a TWIC, as well as individuals applying for an HME. The terms "date of service" and "day" are currently listed in the definition section of part 1572, and TSA proposes to move them to § 1515.3 without any change.

"Date of service" means the date of personal delivery; the mailing date shown on a certificate of service; 10 days from the date of mailing, if there is no certificate of service; another mailing date shown by other evidence if there is no certificate of service or postmark; or the date of an electronic transmission showing when the document was sent.

TSA created this definition with mobile workers in mind, to accommodate the use of email or facsimile, and to provide a 10-day period from the date of mailing, rather than 5 or 7 days. The mariners, commercial truck drivers, train crew members, and other workers subject to the threat assessment requirements may travel from the East Coast to the West Coast on a regular basis, or be stationed away from home for days, weeks, or months at a time. We believe this definition makes the appeal process more reasonable for the group of workers affected.

The term "day" used in the NPRM means calendar day and is the same definition being used in part 1572 now.

49 CFR 1515.5 Appeal procedures.

TSA is proposing to use the substantive appeal standards that currently appear in 49 CFR 1572.141 for HME applicants for TWIC applicants, and proposes to expand the suspense deadlines. TSA has found in implementing the HME program that individuals

making a good faith effort to comply with the timelines set forth in 1572.141 have difficulty doing so. Thirty days may not be adequate for workers who travel for extended periods during the month. Therefore, TSA proposes to extend response deadlines from 30 to 60 days in the appeal process.

An individual may appeal an Initial Determination of Threat Assessment if he asserts that he meets all standards for the security threat assessment. For example, if the Initial Determination was based on information indicating the applicant is not lawfully present in the United States, but the applicant is a lawful permanent resident, he can appeal the Determination and provide TSA proof of lawful presence.

Paragraph (b) of this section sets forth the basic mechanics of the appeal process. An applicant initiates an appeal by providing TSA with a written request for the releasable materials upon which the Initial Determination was based, or by serving TSA with a written reply to the Initial Determination. Currently, if an applicant wishes to receive copies of the releasable material upon which the Initial Determination was based, he must serve TSA with a written request within 30 days after the date of service of the Initial Determination. TSA proposes to change this to 60 days after the date of service of the Initial Determination. Under the current provisions, TSA's response is due within 30 days. We propose to change this requirement so that the response would be due in 60 days. In response, TSA cannot provide any classified information, as defined under 6 CFR part 7 (DHS Classified National Security Information), or under E.O.s 12958, as amended by E.O. 13292 (68 FR 15315(Mar. 28, 2003)), and 12968, or any other information or material protected from disclosure by law.

If an applicant wishes to reply to the Initial Determination, we propose that he or she must provide TSA with a written reply within 60 days after the date of service of the Initial Determination or the date of service of TSA's response to the applicant's request for materials. The applicant should explain why he or she is appealing the Initial Determination and provide evidence that the Initial Determination was incorrect. In an applicant's reply, TSA will consider only material that is relevant to whether he or she meets the standards for the security threat assessment. If an applicant does not dispute or reply to the Initial Determination, the Initial Determination becomes a Final Determination of Threat Assessment.

Under paragraph (b)(3) of this section, an applicant has the opportunity to correct a record on which an adverse decision is based. As long as the record is not classified or protected by law from release, TSA will notify the applicant of the adverse information and provide a copy of the record. If the applicant wishes to correct the inaccurate information, he or she must provide written proof that the record is inaccurate. The applicant should contact the jurisdiction responsible for the inaccurate information to complete or correct the information contained in the record. The applicant must provide TSA with the revised record or a certified true copy of the information from the appropriate entity before TSA can reach a determination that the applicant does not pose a security threat.

The Director makes the Final Determination on appeals that involve disqualifying criminal offenses, mental capacity, and immigration status. However, in a case where an Initial Determination of Threat Assessment is based on the applicant's connection to terrorist activity or similar threat under § 1572.107, the Assistant Secretary of TSA

reviews the appeal and makes the Final Determination. TSA has the Assistant Secretary review these cases to provide additional scrutiny because these cases will likely involve a review of classified information that the applicant cannot see. In addition, these applicants are not eligible for waivers if the Initial Determination stands. TSA believes that the review by the Assistant Secretary for these cases provides an additional protection that the agency's Final Determination of Threat is sound.

In considering an appeal, the Director or Assistant Secretary reviews the Initial Determination, the materials upon which the Initial Determination is based, the applicant's reply and other materials or information available to TSA. The Director or Assistant Secretary may affirm the Initial Determination by concluding that an individual poses a security threat. If this occurs, TSA serves a Final Determination of Threat Assessment on the applicant. Also, for cases involving mariners applying for a TWIC, TSA would provide the Coast Guard with the Final Determination. In cases involving HME applicants, TSA serves the licensing State with the Final Determination. For all TWIC applicants, TSA serves FMSC (who is also the Captain of the Port) with Final Determinations of Threat Assessment. DHS believes that the FMSC, as the chief Federal security officer at the port, should be aware of individuals who are denied a TWIC.

The Final Determination includes a statement that the Director or Assistant Secretary has reviewed the Initial Determination, the materials upon which the Initial Determination was based, the reply, if any, and other available information and has determined that the applicant poses a security threat.

There is no administrative appeal of the Final Determination of Threat Assessment. However, as explained below, an applicant may apply for a waiver under

certain circumstances. For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order.

Paragraph (e) sets forth the procedures to follow if TSA determines that the applicant does not pose a security threat. TSA serves a Withdrawal of the Initial Determination on the applicant and a Determination of No Security Threat on the issuing State for an HME applicant and on the Coast Guard when it involves a mariner applying for a TWIC.

Paragraph (f) provides that TSA cannot disclose to the applicant classified information, as defined in section 1.1(c) of E.O. 12958, as amended by E.O. 13292, and section 1.1(d) of E.O. 12968. See also, 6 CFR part 7. TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law, such as Sensitive Security Information (SSI); sensitive law enforcement and intelligence information; sources, methods, means, and application of intelligence techniques; and identities of confidential informants, undercover operatives, and material witnesses.

For determinations under § 1572.107, the finding that an individual poses a security threat will be based, in large part, on classified national security information, unclassified information designated as SSI, or other information that is protected from disclosure by law.

Classified national security information is information that the President or another authorized Federal official has determined, pursuant to E.O.s 12958, as amended, and 12968, must be protected against unauthorized disclosure to safeguard the security of American citizens, the country's democratic institutions, and America's participation

within the community of nations. See 60 FR 19825 (April 20, 1995). E.O.s 12958, as amended, and 12968 prohibit Federal employees from disclosing classified information to individuals who have not been cleared to have access to such information under the requirements of that E.O. See also, 6 CFR part 7. If the Director determines that an applicant who is appealing the intelligence-related check is requesting classified materials, the applicant will not be able to access classified national security information.

The denial of access to classified information under these circumstances is consistent with the treatment of classified information under the Freedom of Information Act (FOIA), which specifically exempts such information from the general requirement under FOIA that government documents are subject to public disclosure. 5 U.S.C. 552 (b)(1).

SSI is unclassified information that is subject to disclosure limitations under statute and TSA regulations. See 49 U.S.C. 114(s); 49 CFR part 1520 as amended by 69 FR 28066 (May 18, 2004). Under 49 U.S.C. 114(s), the Assistant Secretary of TSA may designate categories of information as SSI if release of the information would be detrimental to the security of transportation. Information that is designated as SSI must only be disclosed to people with a need to know, such as those needing to carry out regulatory security duties. 49 CFR 1520.11 as added by 69 FR 28084-5. The Assistant Secretary has defined information concerning threats against transportation as SSI by regulation. See 49 CFR 1520.5. Thus, information that TSA obtains indicating that an applicant poses a security threat, including the source of such information and the methods through which the information was obtained, will commonly be designated SSI or classified information. The purpose of designating this information as SSI is to ensure

that those who seek to do harm to the transportation system and their associates do not obtain access to information that will enable them to evade the government's efforts to detect and prevent their activities. Disclosure of this information, especially to an applicant specifically suspected of posing a threat to the transportation system, is precisely the type of harm that Congress sought to avoid by authorizing the Assistant Secretary to define and protect SSI.

Other pieces of information also are protected from disclosure by law due to their sensitivity in law enforcement and intelligence. In some instances, the release of information about a particular individual or his or her supporters or associates could have a substantial adverse impact on security matters. The release by TSA of the identities or other information regarding individuals related to a security threat determination could jeopardize sources and methods of the intelligence community, the identities of confidential sources, and techniques and procedures for law enforcement investigations or prosecution. See 5 U.S.C. 552(b)(7)(D), (E). Release of such information also could have a substantial adverse impact on ongoing investigations being conducted by Federal law enforcement agencies, by revealing the course and progress of an investigation. In certain instances, release of information could alert co-conspirators to the extent of the Federal investigation and the imminence of their own detection, thus provoking flight.

For the reasons discussed above, TSA will not provide any classified information to an applicant, and TSA reserves the right to withhold SSI or other sensitive material protected from disclosure under law. As noted above, TSA expects that information will be withheld only for determinations based on § 1572.107, which involve databases that list indicators of potential terrorist activity or threats. When the determination is based

on the individual's criminal records, TSA expects that appropriate supporting records most likely can be disclosed to the applicant upon a written request to TSA. With respect to disqualifications based on immigration status, TSA will provide the applicant with the reason for a denial, but may not be able to provide specific documentation on the applicant's alien status.

TSA has the discretion to extend due dates both for an applicant and for the agency during the appeal process. An applicant must provide a written statement of good cause for extending the due date, within a reasonable time prior to the due date at issue. This is consistent with the rules of civil procedure. TSA anticipates that if an applicant is attempting to correct erroneous records or gather documents in support of a waiver request, the individual may need additional time for the appropriate governmental agency or entity to produce the documents. As long as the applicant provides a sufficient explanation of these problems, TSA will extend the time needed to complete the process. There are a variety of reasons or events that might require an extension of time, and TSA will review these requests liberally to give applicants as much time as is necessary to provide the correct information. Family needs and emergencies, business travel, extreme weather conditions, and lost documents are all considered legitimate reasons on which TSA would grant an extension of time to an applicant. In addition, an applicant's extension request does not have to be a formal document. A handwritten request for an extention of time in a letter to TSA is all that is required. The appeal process is designed for applicants to use without legal counsel and so informal written materials are always accepted.

There are also reasons for which TSA may need to extend a response date, particularly where an applicant is the subject of an ongoing investigation by another agency. This has been a rare circumstance with the hazmat threat assessment process, but it has occurred and undoubtedly will occur with TWIC applicants. TSA is not required under the hazmat rule or in this proposed rule, to provide notice to an applicant that TSA's response may be late. However, applicants may contact TSA to determine the status of an appeal. In the hazmat threat assessment process, TSA has an 800-number for drivers to call to ask questions about the appeal procedures and the status of a particular threat assessment. Typically, TSA is able to provide the requested information within one business day. This process will also be available for TWIC applicants.

Paragraph (i) of this section describes the procedure for appealing an immediate revocation of an HME under § 1572.13(a) or immediate invalidation of a TWIC under § 1572.21(d)(3). Immediate revocation occurs where TSA determines during the course of conducting a security threat assessment that sufficient factual and legal grounds exist to warrant immediate revocation of the HME. For a hazmat driver under these circumstances, the applicant must surrender the endorsement and cease transporting hazardous materials prior to initiating an appeal. For a TWIC, TSA would invalidate the TWIC in the TSA system. TSA understands that removing the individual from service without an opportunity to correct the record may have adverse consequences, but this mechanism will be used only in cases where the risk of imminent danger is significant and the adverse information is highly reliable. This procedure will also be used where an applicant should have surrendered the endorsement or TWIC and/or applied for a waiver, but failed to do so. The individual may appeal this decision, include all supporting

documentation when he or she submits the appeal, and may request releasable documents from TSA.

49 CFR 1515.7 Waiver Procedures.

This section applies to applicants who have been disqualified from holding or obtaining an HME or TWIC due to a disqualifying criminal offense or mental incapacity. The current standard, § 1572.143, applies to HME applicants and provides that an applicant with certain disqualifying offenses or issues of mental competence may apply for a waiver. In this NPRM, TSA proposes to use the same waiver procedures for TWIC applicants. We are providing a discussion of this section to inform TWIC applicants, most of whom did not need to participate in the hazmat rulemaking where these sections were first discussed.

Waivers are offered because an applicant may be rehabilitated to the point that he or she can be trusted in sensitive or potentially dangerous work or has been declared mentally competent. The existing standard and this NPRM provide criteria that TSA considers if the individual does not meet the criminal history standards. TSA believes that these factors are good indicators that an individual may be rehabilitated to the point that a waiver is advisable. The factors are: (1) the circumstances of the disqualifying act or offense; (2) restitution made by the individual; (3) Federal or State mitigation remedies; (4) court records indicating that the individual has been declared mentally competent; and (5) other factors TSA believes bear on the potential security threat posed by an individual. Many of these factors are set forth in MTSA, at 46 U.S.C. 70105(c)(2).

TSA has concluded that some crimes, such as espionage, treason, sedition, a terrorist act, and a crime involving a transportation security incident, are so highly

indicative of a security threat that individuals convicted of them pose an ongoing, unacceptable risk to transportation security. Most likely, these individuals will be incarcerated for a very long term, but the rule now makes clear that convictions for these crimes disqualify an individual for life, with no opportunity to apply for a waiver.

Individuals who are disqualified due to mental incompetence are eligible for a waiver. To support the waiver request TSA will accept a court order or official medical declaration showing that an individual previously declared incompetent is now competent. Generally, TSA will not grant waivers on the basis of a letter from a treating physician stating that the individual is capable of maintaining a job, because these submissions tend to be very subjective and vague. The standard in the rule states that an applicant is mentally incompetent if a court declares it or he or she is involuntarily committed to a mental hospital. Official documents that reverse these findings are necessary for TSA to grant a waiver.

TSA, however, does not grant waivers from the standards concerning immigration status or information discovered during a search under § 1572.107. With respect to immigration violations and findings under § 1572.107, individuals may appeal an Initial Determination based on assertions that the underlying records are incorrect, the applicant's identity is mistaken, or TSA's analysis of the records is not correct. However, if TSA finds that the Initial Determination is accurate, the individual is ineligible for a waiver.

After reviewing an individual's application for a waiver, TSA sends a written decision to the individual. If the waiver is granted, TSA sends a Determination of No

Security Threat to the licensing State or Coast Guard within 60 days after the date of the individual's waiver application.

TSA proposes to add new requirements to paragraph (c) of this section to apply to HME and TWIC applicants. As originally conceived, HME applicants who know they have a disqualifying criminal conviction could apply to TSA for a waiver without initiaing the HME threat assessment process. Therefore, the applicants did not provide all of the biographic information or fingerprints required to conduct a full background check under Part 1572 or pay the full fee for the HME background check. However, in practice TSA would conduct a full background check in order to assess the waiver application properly. Under these conditions, TSA would not possess the best information about the applicant on which to base a waiver decision and did not recover the cost of completing the background check from the applicant. To ameliorate this situation, we propose to require all applicants who know they will be disqualified under the standards in Subpart B of part 1572 and want to apply for a waiver to undergo a full threat assessment for the HME or TWIC and pay all fees associated with the complete security threat assessment. TSA will be able to review all available information in considering an application for a waiver. TSA reviews these materials to ensure that the waiver applicant is being truthful concerning past criminal history and other pertinent activity before determining whether a waiver request should be granted. By requiring the fee and critical biographical information in the waiver submission, TSA will complete waiver evaluations more quickly and effectively. Otherwise, TSA must contact the waiver applicant to request additional information, wait for the information to be submitted and run the risk of missing critical information.

Finally, if legislation is enacted after publication of this proposed rule that would require TSA to adopt a program in which Administrative Law Judges may be used to review cases in which TSA has denied a waiver request, or other changes that would impact the waiver process, TSA will amend the final rule as appropriate to address such statutory mandates.

49 CFR Part 1570 Land Transportation Security: General Rules.

49 CFR 1570.3 Terms used in this part.

TSA proposes to move the definitions of the terms used for the security threat assessment standards from part 1572, Credentialing and Background Checks for Land Transportation Security to part 1570, Land Transportation Security: General Rules. Most of the terms have been through notice and comment in the hazmat rulemaking. TSA proposes to add definitions for terms used in the TWIC standards and amend some of the terms first promulgated in the hazmat rule.

We propose to change the definition of "applicant" to cover individuals who apply for any security threat assessment described in Subchapter D, rather than just individuals who apply for an HME.

The term "Determination of No Security Threat" is amended to clarify that such determinations apply both to the authorization to transport hazardous materials and to unescorted access to secure areas of maritime facilities and vessels. Also, TSA is amending the definition to add that TSA will notify the Coast Guard when issuing a Determination of No Security Threat for a mariner applying for a TWIC.

The definition for "explosive or explosive device" was published in the current hazmat rule at § 1572.3. TSA proposes to move the definition to § 1572.103 to make

clear that the definition applies only to the term as it is used in the list of disqualifying criminal offenses. After publishing the hazmat rule in November 2004, TSA received comments asserting that the definition created confusion between the "explosives" that are hazardous materials under the federal hazardous material regulations and require placarding in transportation, and the crimes that involve explosives and are disqualifying. To resolve these questions, the definition now clearly applies only to § 1572.103, disqualifying criminal offenses. The kind of explosives offenses that are disqualifying are in 18 U.S.C. 232(5), 841(c)-(f), and 844(j), and a destructive device is defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f). The explosive material that requires placarding and triggers the requirement to obtain an HME continues to be defined in regulations issued by the U.S. Department of Transportation. 49 CFR 172.101.

TSA proposes to amend "Final Determination of Threat Assessment" to add that TSA will notify the Coast Guard when TSA determines that a mariner applying for a TWIC does not meet the security threat assessment standards. A Final Determination may not be administratively appealed.

TSA proposes to amend "Initial Determination of Threat Assessment" to also apply to issuance of a TWIC. An Initial Determination may be administratively appealed.

TSA proposes to amend "Initial Determination of Threat Assessment and Immediate Revocation" to extend it to the TWIC threat assessment process. This is an initial administrative determination that an applicant poses an imminent security threat and immediate revocation of an HME or TWIC is necessary. Applicants may appeal the determination after revocation has occurred. TSA issues an Immediate Revocation only

where we believe the driver may pose an imminent threat to transportation, national security, or other individuals. This definition is provided to distinguish the notification documents used in an immediate revocation from the more common Initial Determination process.

"Invalidate" means the action TSA takes when a TWIC is reported as lost, stolen, damaged, no longer necessary, or TSA determines the holder poses a security threat. This action makes the credential inoperative in access control systems.

TSA proposes to definition for the term "owner/operator" to refer to the maritime facilities and vessels subject to MTSA.

TSA proposes to delete the term "pilot state" from the definitions section because the process in which it was used is no longer in effect.

The definition for "revoke" or "revocation" is being amended to apply to the TWIC process as well as the HME process. It is the action TSA or a State takes to cancel, rescind, suspend, or deactivate an HME or TWIC when TSA determines that an applicant does not meet the security threat assessment standards set forth in § 1572.5.

TSA proposes to add a new term, "secure area," which means the area on a vessel, maritime facility, or outer continental shelf facility where security measures have been implemented in a security plan approved by the Coast Guard. For purposes of TWIC, the secure area is the area in which a TWIC is required, unless under escort.

We propose to add a new term, "sensitive security information" to the definition section. This term means information that is described in and must be managed pursuant to the requirements codified at 49 CFR 1520.

TSA is adding language to the definition of "transportation security incident" to reflect a new requirement in SAFETEA-LU. The statute requires TSA to make clear that a transportation security incident does not include work stoppage or other nonviolent action taken in an employee/employer dispute. Therefore, employees or employers who participate in a strike or other labor/management activity cannot be deemed to have committed a disqualifying offense under § 1572.103. TSA is also moving the definition to § 1572.103 to help clarify the kind of crime that is considered disqualifying.

TSA proposes to add a new definition for "transportation worker identification credential." The TWIC is a Federally-issued biometric credential that TSA issues to an individual who has successfully completed a security threat assessment.

TSA proposes to add a new definition for "TSA system" to explain the electronic program used to sort, store, and send security threat assessment information to the appropriate database or enrollment center.

49 CFR 1572 Credentialing and Background Checks for Land and Transportation Security.

49 CFR 1572.5 Scope and standards for hazardous materials endorsement security threat assessment.

This section describes the individuals and entities subject to the requirements in Subpart A and the standards they must meet. In addition, the general standards TSA uses to assess an individual in a security threat assessment.

Subpart A applies to State agencies responsible for issuing commercial drivers licenses and HMEs, applicants who hold or apply for an HME, and applicants who hold or apply for a TWIC.

The security threat assessment standards TSA applies to HME applicants and proposes to apply to TWIC applicants are established by statute. The USA PATRIOT Act and MTSA require TSA to review relevant criminal history, immigration status, and other watch lists and databases that TSA believes appropriate to make an informed security assessment. An applicant poses a security threat if convicted of certain serious crimes, is not lawfully present in the United States, has a connection to terrorist activity, or has been adjudicated as lacking mental capacity. The specific criteria TSA reviews to determine whether an applicant poses a security threat is described in Subpart B and is discussed in detail below.

We are proposing to add paragraph (d) to this section to establish a process by which TSA can determine if a security threat assessment completed by another government entity is comparable to the assessment required in part 1572. As noted above, SAFETEA-LU established several mandates for TSA concerning security threat assessment, one of which we address in this section. TSA must initiate a rulemaking to address the comparability of Federal background checks and eliminate redundant checks. TSA proposes to consider checks conducted by Federal, State, and local governmental bodies in the comparability assessment. TSA will evaluate all aspects of the agency threat assessment, including checks of relevant criminal history databases, immigration status, relevant intelligence and international databases, duration, identity verification and authentication, and the use of biometrics for credentialing.

It is important to note that TSA must adhere to its own security standards in evaluating other threat assessments. TSA intends to make a determination of comparability only where it is clear that the threat assessment of the agency applying for

the determination includes all of the critical components of TSA's check. Many governmental bodies focus on factors that relate specifically to the work done by the agency when conducting a background check and therefore would not necessarily include a check of intelligence data or immigration status. Similarly, local and State agencies might not have conducted terrorist database checks. TSA most likely cannot issue a positive comparability determination in these cases.

The age of the threat assessment is another area that TSA will review carefully. For purposes of the threat assessment standards set forth in part 1572, a new threat assessment is required every five years. If TSA determines that another security threat assessment is comparable to part 1572 checks, then we must determine how long the check remains valid. For the most part, all checks would have to be renewed every five years. However, there may be circumstances under which the check would remain valid for a longer or shorter term, depending on other factors surrounding the breath of the threat assessment, such as whether perpetual checks are part of the assessment.

TSA plans to establish a verification process between TSA and participating agencies to ensure that only employees who have successfully completed a threat assessment through another agency are approved under TSA's comparability determination. TSA will strive to automate the verification process to reduce costs and processing time. TSA will establish rules governing the exchange of information between TSA and the participating agency, including appropriate Interface Control Documents (ICD). TSA may enter into Memoranda of Understanding (MOU) with other agencies if necessary.

TSA plans to notify the public of any determinations of comparability, unless otherwise prohibited by law or such a disclosure would reveal sensitive security information. TSA considered proposing that individuals, rather than agencies, could apply for a comparability determination, but has determined that the costs would increase substantially and the reliability of the information exchanged could be questionable. TSA proposes to notify the public when comparability determinations are made, to make certain that all individuals who are eligible are aware of the determination.

An applicant who completes a threat assessment that TSA determines to be comparable to the assessment set forth in part 1572, and wishes to apply for a TWIC to gain unescorted access to a secure area of a facility or vessel, would have to complete the enrollment process required for a TWIC and pay the corresponding fee to cover the cost of information collection and issuance of the credential. However, because a duplicate threat assessment would not be required, the applicant would not have to pay a threat assessment fee.

In making comparability determinations, TSA proposes to "grandfather" the comparable threat assessment for the period of time remaining before that threat assessment would expire. For instance, if an HME holder completed the threat assessment under part 1572 in October 2005 and applies for a TWIC in October 2006, TSA would issue the TWIC for the period of time remaining before the HME threat assessment expires. Therefore, the TWIC would show an expiration date of October 2010 – five years from the date of the HME threat assessment.

TSA proposes to announce comparability determinations in this NPRM. First, an applicant who successfully completes the security threat assessment required for an HME

would be deemed to have completed the threat assessment for a TWIC. The standards and period of validity are the same for an HME and a TWIC. However, if an HME holder wishes to apply for the TWIC credential to have unescorted access to secure areas of a facility or vessel, the applicant would complete the TWIC enrollment process and provide the biometric information for issuance of the credential.

Second, TSA deems the security threat assessment required to obtain a FAST card, as part of the Free and Secure Trade program administered by U.S. Customs and Border Protection (CBP), an agency within DHS, to be comparable to the security threat assessment set forth in part 1572. FAST is a cooperative effort among CBP and the governments of Canada and Mexico. Applicants from Canada, Mexico, and the United States may volunteer to undergo a background records check and if they complete it successfully, may receive expedited entrance privileges at the northern and southern borders, subject to other requirements. CBP conducts a fingerprint-based criminal history records check, name-based checks of pertinent intelligence databases, and a personal interview. Canada conducts a similar check for Canadian citizens. The FAST card and background check are valid for five years.

TSA invites comment on paragraph (d) from all interested parties. TSA invites other agencies and workers who may be affected by this section to propose different or additional standards to make this process as efficient and effective as possible. TSA urges all agencies interested in obtaining a comparability determination to contact TSA, not only with comments to the proposed rule, but also to inform TSA of the interest in seeking the determination. Please contact Assistant Program Manager, Attn: Federal

Agency Comparability Check, Hazmat Threat Assessment Program, TSA-19, TSA, 611 South 12th Street, Arlington, VA 22202.

49 CFR 1572.7 Waivers of security threat assessment standards.

This section describes the TWIC applicants who TSA proposes may apply for a waiver of the threat assessment standards. As we do with HME applicants, TSA proposes that TWIC applicants who have been convicted of certain criminal offenses and those who have been declared mentally incompetent in the past may apply for a waiver. Individuals convicted of treason, sedition, espionage, a crime involving a transportation security incident, and a crime of terrorism are not eligible for a waiver from TSA. TSA believes this is appropriate given the severity and level of risk these crimes reflect. For applicants who do not meet the immigration standards in § 1572.105, there is no circumstance or set of facts under which TSA would wish to suspend the application of the lawful immigration categories listed to issue a waiver. Additionally, if a TWIC applicant is disqualified under § 1572.107, the applicant should not be eligible for a waiver. Granting a waiver to an individual determined to pose a security threat would undermine the purpose of this rule and the statutes that gave rise to it.

49 CFR 1572.9 Applicant information required for security threat assessment for a hazardous materials endorsement.

This section describes all of the identifying information an HME applicant must provide in order for TSA to complete the fingerprint- and intelligence-related checks. TSA is proposing one change in paragraph (g) relating to employer notification of adverse threat determinations. TSA proposes to add a statement to the application process, informing the applicant that TSA may notify the applicant's employer if TSA

determines that he or she poses a security threat. TSA believes that applicants should be fully aware of TSA's authority and responsibility to provide employer notifications at the time of the threat assessment application.

49 CFR 1572.11 Applicant responsibilities for a security threat assessment for a hazardous materials endorsement.

This section describes the standards with which each HME applicant must comply and the actions the applicant must take in order to hold an HME. TSA is not proposing any changes to this section.

49 CFR 1572.13 State responsibilities for issuance of hazardous materials endorsement.

This section lists all of the responsibilities that the States must perform in order to ensure that only individuals who meet the security threat assessment standards receive a hazmat endorsement. TSA is not proposing any substantive changes to this section, except to remove sunset provisions. Former paragraph (b) included compliance dates that have passed and so are not necessary to reference in rule text. Former paragraph (c) permitted a State to apply to be a "Pilot State" prior to January 31, 2005 and is no longer necessary. Former paragraph (f) required States to submit a declaration by December 27, 2004 if the State wanted to conduct fingerprint collection, and is no longer necessary.

49 CFR 1572.15 Procedures for security threat assessment for an HME.

TSA is not proposing to make any changes to this section. This section describes the security threat assessment process in detail, and provides that no State can issue an HME unless the steps outlined in this section have been completed.

49 CFR 1572.17 Applicant information required for the security threat assessment for TWIC.

TSA is proposing this new section to require TWIC applicants to provide biographic and biometric information necessary for TSA to conduct a comprehensive security threat assessment. This proposed section is nearly identical to § 1572.9, Applicant information required for the security threat assessment for an HME. However, in this section, TSA proposes to require the applicant to explain his or her need for a TWIC. Paragraph (a)(10) states that the applicant must provide his or her job description and the facility, vessel, or port where the applicant requires unescorted access, if it is known. Paragraph (a)(11) asks for information concerning the applicant's employer, if known. Paragraph (f) proposes to require each TWIC applicant to certify that he or she needs unescorted access to secure areas of maritime facilities as part of their employment duties, or that he or she is a merchant mariner.

TSA is proposing these requirements to limit TWIC to individuals with a legitimate need to enter secure areas of maritime facilities. First, TSA has authority to conduct threat assessments on individuals only in furtherance of its transportation security authorities. We cannot conduct security threat assessments on persons who have no such nexus. This principle is consistent with security standards in other modes of transportation. For instance, in aviation, each airport operator determines which individuals need unescorted access to the secure area of the airport, and the airport conducts a background check and provides a credential to those individuals. TSA has no employment or business relationship with the TWIC applicant and so we propose to obtain a minimum level of information from the applicant to avoid conducting security

threat assessments and providing a tool for accessing facilities to any individual who may have a criminal motive or casual interest in the facility. Ultimately, the facility owner controls the individuals that are given unescorted access through the access control system, but TSA believes some sort of minimal filter is advisable to restrict TWIC to those who have a need for it. TSA also believes this may prevent an unscrupulous employer who has no connection to a facility or vessel from using the TWIC threat assessment process as a free suitability assessment in making hiring decisions. TSA does not intend for this provision to adversely impact an employee who is seeking employment in the maritime industry and applies for a TWIC to increase his or her marketability. These applicants should be able to articulate the facility, vessel or port where they may seek employment, which would satisfy paragraph (a)(10).

49 CFR 1572.19 Applicant responsibilities for a security threat assessment for TWIC.

In this section, we propose the basic duties a TWIC applicant must comply with to satisfy the rule. Paragraphs (a) and (b) propose a timeline for enrollment for TWIC applicants. As currently envisioned, enrollment of the current population subject to this rule will be accomplished three phases:

	Start Date	End Date
Group 1	Effective date of rule.	Not later than 10 months after effective date of rule.
Group 2	After Group 1.	Not later than 15 months after effective date of rule.
Group 3	After Group 2.	Not later than 18 months after effective date of rule.

We believe that a staggered rollout is the most efficient way to implement a program of this size and complexity. TSA and the Coast Guard plan to focus resources

consistent with the schedule above and complete each grouping as quickly as possible. The length of the enrollment period at each port will vary depending on port population, with the requirement that enrollment at all regulated facilities and vessels must be completed within 18 months after the effective date of the final rule. TSA and Coast Guard also are contemplating implementing a more flexible rollout, with anticipated dates to be announced by notices published in the Federal Register. The timetable proposed in the rule does not include actual credential issuance. Once the enrollment process is complete for an applicant, the time required to complete the threat assessment and have the credential ready to issue will typically be 30 days.

As proposed, each FMSC, with input from the AMS Committee, would establish his/her own plan for scheduling enrollment to ensure a steady flow of enrollees, prevent long lines, and avoid disrupting commerce. TSA plans to establish enrollment times that are consistent with normal port operations. To allow flexibility and service the maritime population effectively, TSA will deploy permanent and mobile enrollment centers. Enrollment workstations will be fielded at larger ports in sufficient quantity to complete the enrollments within the required timeframe, assuming reasonably steady enrollment rates. The strategic placement of the enrollment stations will accommodate port management and operational requirements, and satisfy new enrollments and replacement of lost or stolen credentials.

Paragraph (b) of this section discusses the enrollment of mariners. Mariners who hold an MMD or License can enroll in TWIC pursuant to the schedule in paragraph (a). However, these applicants are not required to undergo the criminal history records portion of the TWIC security threat assessment if they received an MMD after February

3, 2003 or a License after February 13, 2006. These applicants must provide the information necessary for enrollment, including biometric information, and obtain the credential. These MMD and License applicants have completed a full security background check performed by the Coast Guard, including review of criminal records for all crimes listed in 46 CFR 10.201 or 46 CFR 12.02-4. These include terrorism offenses, acts of sabotage, and espionage. In addition, the Coast Guard safety and security evaluation analyzes several data sources that contain intelligence information and includes a verification of immigration status.

We have agreed to eliminate the requirement for a criminal history records check for this portion of the merchant mariner population to prevent redundancy and reduce costs for applicants and the government. Mariners who have already had their background fully vetted by the Coast Guard are not required to undergo the full TWIC security threat assessment described in part 1572 for their first TWIC, as long as their MMD or License is current. TWICs issued in accordance with these procedures will expire five (5) years after the date of the Coast Guard security threat assessment, and align with the expiration date of the MMD or license, as applicable. Although a mariner may opt to undergo the full security vetting and be issued a TWIC that is valid for the full 5-year period, this is not required for the mariner population who have an MMD issued after February 3, 2003 or a License issued after January 13, 2006.

In paragraphs (c)-(e) we propose the same standards that currently apply to HME applicants. TWIC holders would be required to surrender the TWIC to TSA if TSA determines that the holder poses a security threat, and have a continuing obligation to report a disqualifying event to TSA. In addition, TWIC applicants would be required to

submit the biometric and biographic information required in § 1572.17 and the security threat assessment fee to TSA once every five years.

Paragraph (f) addresses lost, stolen, or damaged credentials. To minimize fraud and prevent unauthorized individuals from entering the secure areas, TWIC holders must report lost or stolen credentials to TSA as soon as the holder loses possession of the credential. TSA would then invalidate the credential number in the TSA system to prevent it from being used in an access control system. Employees will pay a fee for the cost of the replacement credential, but we do not currently plan to require a new threat assessment. The expiration date on the replacement credential will be the same as the expiration date on the original card.

If a TWIC holder finds that the credential no longer operates as intended in the access control system, he or she should report it and go to an enrollment center to determine the cause of the malfunction. Unless there is an inherent defect in the credential, the holder will be charged a fee of $36 for a replacement credential.

49 CFR 1572.21 Procedures for security threat assessment for a TWIC.

This section outlines the procedures TSA, applicants, and owners/operators would follow in completing the security threat assessment. These procedures are nearly identical to the procedures followed in the HME process. However, where TSA notifies a State of a Final Determination of Threat Assessment, Determination of No Security Threat, or an Immediate Revocation in an action involving an HME, TSA would notify the Coast Guard with respect to a TWIC applicant who is a mariner. TSA provides this information to the Coast Guard because TSA's final determination bears on the mariner's credential. If the mariner is not eligible for a TWIC, the Coast Guard will not issue the

mariner credential. Also, TSA will notify the FMSC of TWIC revocations and denials. As the chief governmental security officer at a port, the FMSC should be aware of an applicant who is denied a TWIC or has a TWIC that has been revoked.

49 CFR 1572.23 Conforming equipment; Incorporation by reference.

Each owner/operator required to have access control systems and equipment, including card readers, in conjunction with TWIC, must meet TSA-approved standards. These readers shall conform to referenced industry standards employed by TSA for secure identity credentials. TSA plans to incorporate these standards by reference in the final rule. These standards are listed in proposed § 1572.23. Copies of these standards may be obtained through the Web sites and addresses listed in proposed § 1572.23.

49 CFR 1572.24-40 [Reserved].

49 CFR 1572.41 Compliance, inspection and enforcement.

In this section, TSA proposes standards requiring owners/operators to permit TSA personnel to enter the secure areas of maritime facilities to evaluate, inspect, and test for compliance with the standards in part 1572.

These proposals are standard and necessary for TSA to exercise its oversight and enforcement responsibilities over trusted agents, the enrollment process, and the performance of the credential in a variety of circumstances. TSA will be subject to audits and reporting requirements on the TWIC threat assessment and credentialing system that require visual and operational assessments that necessitate access to facilities and vessels. TSA will work cooperatively with owners/operators to minimize adverse impacts on normal operations.

49 CFR 1572.101 Scope.

TSA is amending this section to add TWIC applicants to the group of individuals subject to the threat assessment standards. Also, TSA is adding paragraph (a) to this section to acknowledge that hazmat drivers are subject to additional standards issued by the Federal Motor Carrier Safety Administration and the State that issues the commercial driver's license, including safety requirements, immigration status and criminal history standards.

49 CFR 1572.103 Disqualifying Criminal Offenses.

TSA proposes to adopt the list of criminal acts that disqualify an applicant from holding an HME under 49 CFR 1572.103 for TWIC applicants. In addition, TSA proposes to make one substantive and several administrative changes to this section, as it applies to HME and TWIC applicants. TSA is moving the definitions of "explosive," "firearm," and "transportation security incident" from § 1572.3 to § 1572.103, where the terms are used. This should help to eliminate uncertainty about the crimes that are disqualifying. In addition, TSA is adding clarifying language concerning the kind of activity that constitutes a 'transportation security incident.' As required in SAFETEA-LU, the definition now makes clear that nonviolent labor-management activity is not considered a disqualifying offense. TSA also adds paragraph (a)(1) to the scope of this section acknowledging that hazmat drivers are subject to other standards issued by the Federal Motor Carrier Safety Administration and the State that issues the driver's commercial license and hazmat endorsement.

TSA is proposing a substantive change to this section concerning the crimes of treason, sedition, espionage, and terrorism listed in § 1572.103(a), which are permanently

disqualifying. Applicants convicted of these crimes are not eligible for a waiver. TSA is adding conspiracy to commit these crimes to the list of crimes that are not subject to a waiver request. TSA has determined that a conviction of conspiracy to commit espionage, treason, sedition, or terrorism are indicative of a serious, ongoing, unacceptable risk to security and should not be waived under any circumstances. This change applies to HME and TWIC applicants.

Paragraph (d) describes how an arrest with no indication of a conviction, plea, sentence or other information indicative of a final disposition must be handled. TSA proposes to change the time allowed for an applicant to provide correct records from 30 days to 60 days. The individual must provide TSA with written proof that the arrest did not result in a conviction of a disqualifying criminal offense within 60 days after the date TSA notifies the individual. If TSA does not receive such proof in 60 days, TSA notifies the applicant that the he or she is disqualified from holding an HME or a TWIC.

TSA is considering whether to change the list of disqualifying criminal offenses and invites comment on this matter. TSA received comments on this list following publication of the November 2004 hazmat rule, particularly concerning crimes with explosives. Commenters suggested that possession of explosives should not be disqualifying if the conviction results from previous criminal activity, perhaps nonviolent, that makes any subsequent possession of an explosive or firearm a felony. Also, commenters suggested that explosives convictions should be disqualifying only when the crime involves explosives in the amount and packaging that require placarding in transportation.

Even assuming TSA agrees with these suggested changes, the current criminal recordation system does not include the level of detail these distinctions require. Often, criminal rap sheets list only the statute violated, which may or may not include "explosives" in the title. Rarely, if ever, would a rap sheet include specific facts about the amount or type of explosive involved, or whether the conviction is based on a previous underlying conviction that prohibits contact with explosives. These are the kind of facts TSA can and does evaluate during a request for a waiver, where the applicant provides background information surrounding the conviction and any mitigating information. TSA invites comment on this and any other issue related to disqualifying criminal offenses, in which the public believes TSA can improve the process.

TSA may amend § 1572.103 as it applies to TWIC and HME applicants. Any amendment to the list of disqualifying crimes will apply equally to TWIC and HME applicants.

49 CFR 1572.105 Immigration status.

The immigration standards in this section currently apply to HME applicants, with the exception of paragraph (a)(2)(iv), which is a new proposal. TSA now proposes to apply the entire section to TWIC applicants.

TSA proposes to add a new paragraph to permit certain drivers licensed in Canada or Mexico who frequently deliver goods to facilities and vessels to meet the immigration standards for holding a TWIC. These drivers are admitted to the United States under a North American Free Trade Agreement (NAFTA) implementation visa category. 8 CFR 214.2(b)(4)(i)(E). These drivers are lawful non-immigrants, doing business in the United States, but are not "working in" the United States for purposes of

the immigration laws. These individuals do not possess (nor are they required to possess under this particular visa category) specific documentation authorizing them to work in the United States for a specified time, as is required of other lawful nonimmigrants applying for a TWIC under paragraph 1572.105(a)(3)(i)-(iii). This proposed paragraph is intended to cover the significant number of commercial drivers regularly entering the United States to deliver food and other products to a port or vessel. Requiring these drivers to enter the access control portion of the port under escort would interfere with normal port operations and could potentially adversely affect other businesses on the port. This proposal would not have any impact on existing requirements that must be met to receive a visa under 8 CFR 214.2(b)(4)(i)(E).

TSA invites comment on this proposal from all interested parties.

49 CFR 1572.107 Other analyses.

This section of TSA's HME rule currently applies to HME applicants and we are proposing to apply it to TWIC applicants. MTSA requires that TSA disqualify an individual that "poses a terrorism security risk to the United States." For checks under this section for the HME process, TSA accesses relevant international databases, such as Interpol-U.S. National Central Bureau, and other appropriate sources of information on terrorists and terrorist activity, violent gangs, fugitives from justice, and international criminal records. These sources are also appropriate for TWIC applicants.

Paragraph (c) states that TSA may determine that an individual poses a security threat if TSA's search reveals an extensive or very serious domestic or foreign criminal history, conviction for serious crimes not listed in § 1572.103, or an extensive period of imprisonment, foreign or domestic, exceeding 365 consecutive days. TSA placed this

language in the hazmat rule to clarify the full application of this section and to provide sufficient notice to the public that there may be cases in which an applicant's criminal record includes convictions for serious crimes that are not specifically listed in § 1572.103, but may be disqualifying. Also, if an applicant has been imprisoned for more than a year, which is generally indicative of a serious offense or a long history of criminal activity, TSA may determine that the applicant poses an unacceptable security threat.

As TSA noted in the hazmat rulemaking, we cannot possibly list all of the offenses or other information that may be relevant to determining whether an individual poses a security threat that warrants denial of an HME. TSA has discretion to carry out the intent of MTSA and the USA PATRIOT Act and assess threats to transportation and the Nation, where the intelligence and threats are so dynamic. TSA understands that the flexibility this language provides must be used cautiously and on the basis of compelling information that can withstand judicial review. TSA invites comment on this section.

49 CFR 1572.109 Mental capacity.

The explosives laws prohibit individuals who have been adjudicated as lacking mental capacity from transporting explosives. The hazmat rule currently provides that any person who has been determined to lack mental capacity does not meet the standards for a security threat assessment. We propose to extend this qualification standard to TWIC applicants.

An individual lacks mental capacity, for purposes of this NPRM, if he or she has been committed to a mental health facility or has been adjudicated as lacking mental capacity. An individual is adjudicated as lacking mental capacity if a court or other

appropriate authority determines that the individual is a danger to himself or herself, or lacks the mental capacity to manage his or her affairs. An individual is "committed to a mental health facility" if formally committed by a court; this term does not refer to voluntary admissions to a mental institution or hospital.

Subpart E Fees for Transportation Worker Identification Credential.

A. TWIC Maritime Population Estimation Methodology

TSA conducted an analysis of the maritime population to determine the necessary fee level for the TWIC threat assessment, including enrollment; adjudication, appeals and waivers; and issuance of the credential. TSA estimates that during initial rollout of the program, it will issue TWIC credentials to approximately 750,000 workers requiring regular, unescorted access to secure areas of MTSA-regulated facilities. This figure is the product of survey and analysis work by TSA and Coast Guard personnel, using information provided by individual ports, public and private-sector data sources, interviews with sector subject-matter experts, and extrapolation from survey responses.

In developing this estimate, TSA first identified a wide array of worker categories at MTSA-regulated facilities that would most likely to be required to carry a TWIC. This list evolved during the course of TSA's rulemaking process, both to reflect new information as well as consultations with Coast Guard and maritime industry representatives. The list of major port-related personnel subject to TWIC requirements is as follows:

- Cruise Workers (Land-Based Only)
- Liquid Bulk Refining/Processing Workers
- Longshoremen
- Merchant Mariner Document or License Holders
- Off-Shore Liquid Bulk Workers (i.e. MODUs)
- Rail Workers
- Shipyard Workers

- Site Management/Administration Workers
- Truck Drivers
- Vessel Operations/Port Support Workers
- Contractors/Other

The 750,000 figure was derived from analyzing each of these employment segments using a number of approaches and resources. First, TSA and Coast Guard conducted a maritime population survey during late 2004 and early 2005. TSA and Coast Guard interviewed management officials from 45 ports across the United States, covering many of the nation's largest cargo operations.[5] We asked senior port managers and security officers to estimate the number of workers requiring regular unescorted access to their ports, subdivided into distinct employment categories. To enable comparisons between ports and estimate the range of labor required to load/unload/transport a specific volume of freight, port officials also estimated tonnage and twenty-foot equivalent units (TEU) statistics by cargo type for their ports, such as container, liquid bulk, dry bulk, and roll-on/roll-off ("ro-ro").

This data was utilized to generate four geographically-diverse extrapolation scenarios, each approximating the nationwide distribution of different cargo types.[6] TSA and Coast Guard used this approach to minimize the impact of the significant variation it found in labor intensiveness across ports, and to incorporate a broader array of port data in TSA's calculations. TSA and Coast Guard believe that this method yielded reliable port worker population estimates in the following categories:

---

[5] Ports surveyed (in whole or in part) include: Baltimore, Beaumont, Boston, Brownsville, Brunswick, Burns Harbor, Charleston, Cleveland, Duluth-Superior, Gulfport, Houston, Jacksonville, Lake Charles, Long Beach, Los Angeles, Miami, Milwaukee, Mobile, Morehead City, New Orleans, New York/New Jersey, Oakland, Palm Beach, Panama City, Pascagoula, Pensacola, Philadelphia, Port Arthur, Port Canaveral, Port Hueneme, Port Manatee, Portland (ME), San Diego, San Francisco, Savannah, Seattle, South Louisiana, Tampa, Texas City, Toledo, Virginia Ports (Newport News, Norfolk, Portsmouth), Wilmington (DE), and Wilmington (NC).

[6] The TSA Office of Revenue and MARAD representatives jointly cooperated on a cargo type interpretation of U.S. Army Corps of Engineers Waterborne Commerce data, producing a single

- Site Management/Administration (70,000)
- Vessel Operations/Port Support (50,000)
- Rail (10,000)
- Contractors/Other (70,000)

TSA and Coast Guard also used industry-based employee research to complement the maritime population survey. The agencies believe that the survey did not produce sufficiently accurate worker counts for longshoremen and port truckers in particular, because employees in these classes sometimes work at multiple facilities and thus were likely double-counted in the TSA/Coast Guard survey data. For this reason, industry-wide estimates of port truckers and longshoremen were substituted for the agencies' initial survey data involving these sectors.

The total longshoremen estimate (60,000) was reached by aggregating data from labor unions and port management organizations.[7] The port trucker estimate (110,000) was developed using the 2002 (latest available) Vehicle Inventory and Use Survey (VIUS) of the US Census Bureau, isolating respondent populations with common port container trucker characteristics. Additionally, an estimate for non-container drivers was based on a consensus percentage of the total VIUS survey data from trucking subject-matter expert interviews.[8] [9]

TSA and the Coast Guard also conducted employment category research with leading maritime associations and other relevant organizations to account for MTSA-regulated maritime

---

normalized basis for extrapolation projections: 49% liquid bulk, 9% container, 41% dry bulk/break bulk, 1% ro-ro.

[7] Sources consulted by TSA include the Pacific Maritime Association, United States Maritime Alliance, International Longshoreman's Association, and International Longshoremen and Warehouse Union.

[8] Sources consulted by TSA include (but are not limited to) the American Trucking Association, Owner-Operator Independent Drivers Association, International Brotherhood of Teamsters (Port Division), and academic subject-matter experts from the University of Michigan, University of Minnesota-Morris, and California State University at Long Beach.

[9] According to subject-matter experts consulted by TSA, the vast majority of port truckers (~80%) drive containers. Thus, TSA estimated non-container port truckers to be 20% of the total population. Common characteristics of this sector include: independent owner-operator status, for-hire employment basis, high proportion of short hauls (less than 100 miles).

population segments that the agencies believe were either not represented or under-represented in its maritime population survey. These segments include:

- Barge Operators (30,000)[10]
- Land-Based Cruise Personnel (15,000)[11]
- Liquid Bulk Refining/Processing (80,000)[12]
- MODU/Offshore Liquid Bulk (30,000)[13]
- Shipyard (55,000)[14]

Finally, TSA and the Coast Guard integrated the Coast Guard's operational data for merchant mariners. The National Maritime Center (NMC) – which provides credentialing, training, and certification services to all merchant mariners – lists 204,835 domestic MMD and MML holders.[15] While no reliable data exists on the overlap between MMD holders and active land-based port workers, representatives of NMC and TSA arrived at a rough estimate of 35,000. Thus, the net active estimate for MMDs who will require TWICs is ~170,000 (205,000 – 35,000 overlapping MMDs counted among other categories).

The aggregate results of TSA/Coast Guard maritime employment population research are summarized in the table below:

Maritime Employment Sector	**TSA/Coast Guard Population Estimate**[16]

[10] Based on sector data provided by American Waterways Operators.
[11] Extrapolation based on Maritime Population Survey population data and International Council on Cruise Lines (ICCL) market share information.
[12] MTSA-regulated refinery estimate (35,000-40,000) reflects National Petrochemical and Refiners Association (NPRA) Injuries and Illness Survey data. Other liquid bulk numbers are extrapolations based on MTSA-regulated facility population data in the EPA Risk Management Database.
[13] Based on sector data provided by the Minerals Management Services of the US Department of Interior. Only MTSA-regulated offshore facilities are included.
[14] Based on data provided by MARAD's Office of Shipbuilding and Marine Technology. Sources consulted by TSA include (but are not limited to) the American Shipbuilding Association and Shipbuilders Council of America. Only MTSA-regulated shipyards are included.
[15] Date is as of June 2005. Includes both MMDs and other license holders to be covered by TWIC.
[16] Population estimate is for those persons requiring regular unescorted access to secure areas of MTSA-regulated facilities.

MMD and License Holders	205,000
MMD/License Overlap with Other Worker Categories	-35,000
Port Truck Drivers	110,000
Liquid Bulk Refining/Processing	80,000
Site Management/Administration	70,000
Contractors/Other	70,000
Longshoremen	60,000
Shipyards	55,000
Vessel Operations/Port Support	50,000
MODU/Offshore Liquid Bulk	30,000
Barge Operators	30,000
Land-Based Cruise	15,000
Rail Workers	10,000
Total TWIC Initial Maritime Population	**750,000**

TSA and Coast Guard have set an 18-month TWIC enrollment period for MTSA-regulated facilities and vessels beginning in the final month of FY06, with the majority of enrollments occurring in FY07 and completion by mid FY08. The enrollment plan assumes that workers at the largest U.S. ports are enrolled first, and those at small and rural locations will be completed toward the end of this cycle. TSA estimates a 1% population growth per year, not including worker turnover, in which individuals leave the port worker population and are

replaced by new port workers.[17] Accounting for this annual population growth net of turnover, (or "net population growth")," results in an 18-month initial enrollment population of approximately 758,000.

1. Recurring Population

TSA estimates that approximately 12 percent of port workers will leave the port labor force every year and thus will be replaced by new workers who will require a TWIC. This estimate is derived from TSA and Coast Guard's informal port population survey efforts and related anecdotal evidence. Given that the port population segments discussed above are extremely diverse in operations and demographics, TSA expects this annual turnover will not be consistent across all categories or locations. Assuming a 12 percent annual rate and 1 percent net population growth per year, TSA estimates a five-year total turnover of approximately 410,000.

TSA also estimates that 8 percent of port workers will lose or damage their TWIC credentials each year. This estimate is derived from anecdotal evidence from other Federal credentialing programs. Assuming an 8 percent annual rate and 1 percent net population growth per year, TSA estimates five-year lost/damaged credential totals of some 273,000.

2. Five-year Enrollment Population

Based on these calculations, TSA estimates total five-year TWIC enrollments (initial enrollments, including annual net population growth, plus job turnover enrollments), of approximately 1,168,000. This estimate does not include the lost/damaged card replacement estimate of 273,000 over five years.

[17] Population growth estimate derived from the Bureau of Labor Statistics' (BLS) National Employment Matrix, which estimates growth in the "Transportation and Warehousing" sector of the economy at 1.1 percent

B. Proposed Fee

To comply with the mandates of Section 520 of the 2004 DHS Appropriations Act, TSA proposes to establish user fees for individuals who apply for or renew a TWIC, and thus are required to undergo a security threat assessment in accordance with 49 CFR part 1572. TSA proposes to establish a new user fee (with two components), separate from the fee the FBI charges to check its criminal history records databases.[18]

First, TSA proposes an Information Collection/Credential Issuance Fee to cover the costs of collecting the biometric and biographic information, transmitting the information to the appropriate process or location, and issuing the credential. Second, TSA proposes a Threat Assessment/Credential Production Fee to cover TSA's costs to perform and adjudicate security threat assessments; administer the appeal and waiver process; conduct program oversight; and produce the credential. Third, TSA proposes a fee to cover the cost of creating a new credential to replace a lost, stolen, or damaged credential. Based on the information currently available to the agency, TSA proposes the following fees: an Information Collection/ Credential Issuance Fee ranging from $45 - $65; a Threat Assessment/Credential Production Fee of $50 - $62; and a Credential Replacement Fee of $36. The FBI currently charges a fee of $22 for the criminal history records check, which is also collected whenever a security threat assessment is required.

Pursuant to the Chief Financial Officers Act of 1990, DHS/TSA is required to review these fees no less than every two years. 31 U.S.C. 3512. Upon review, if it is found that the fees are either too high (i.e., total fees exceed the total cost to provide the

[18] The FBI is authorized to establish and collect fees to process fingerprint identification records and name checks for non-criminal justice, non-law enforcement employment and licensing purposes that may be used

services) or too low (i.e., total fees do not cover the total costs to provide the services), the fee will be adjusted. In addition, TSA may increase or decrease the fees described in this regulation for inflation following publication of the final rule. If TSA increases or decreases the fees for this reason, TSA w ill publish a Notice in the Federal Register notifying the public of the change.

1. Information Collection/Credential Issuance

The security threat assessment process requires all applicants who apply for or renew a TWIC to submit their fingerprints and biographic information at a TSA-approved enrollment facility. The same enrollment facility will handle credential issuance to the applicant after successful completion of the threat assessment process. TSA will hire a contractor agent to provide these services. Based on TSA's research of the costs of both commercial and Government fingerprint and information collection services, as well as a prior competitive bidding and acquisition process for similar (but less extensive) services in support of TSA's HME program, TSA estimates that the per applicant cost to collect and transmit fingerprints and other required data electronically is likely to be between $45 and $65. This fee also includes the costs for related administrative support, help desk services, quality control, credential distribution and related logistics.

2. Threat Assessment/Credential Production

For the TSA security threat assessment and credential production process, each applicant's information will be checked against multiple databases and other information sources so that TSA can determine whether the applicant poses a security threat that warrants denial of a TWIC. The threat assessment includes an appeal process for individuals who believe the

---

for salaries and other expenses incurred in providing these services. See Title II of Pub. L. 101-515,

records upon which TSA bases its determination are incorrect. In addition, TSA will administer a waiver process for applicants denied a TWIC due to criminal activity or mental incompetence.

TSA must implement and maintain the appropriate systems, resources, and personnel to ensure that fingerprints and applicant information are appropriately linked, and that TSA can receive and act on the results of the security threat assessment. TSA must have the necessary resources – including labor, equipment, database access, and overhead – to complete the security threat assessment process.

TSA estimates that the total cost of threat assessment services will be $24.1 million over five years. This estimate includes $4.6 million for all information systems expenses, including the modification and sustainment of TSA's Screening Gateway. The Screening Gateway is an information system platform that allows TSA to submit, receive, and integrate security threat assessment information from a variety of Federal, State, and other sources in order to help make security threat assessment determinations.

Upon successful completion of the threat assessment process, the applicant's enrollment record is sent to the TSA-approved credential production facility. The production facility initiates the TWIC credential personalization process, which includes printing and magnetic stripe and chip encoding. Before the credentials are shipped back to the enrollment center, the credential production facility employees perform quality control inspections. TWIC credentials are then securely packaged and shipped to the designated enrollment center.

The credential production process will be administered by a TSA-approved federal credential production facility. It will require expenditures for the following items: card stock, customization materials (i.e., contactless chips, laminates), biennial credential re-design,

---

November 5, 1990, 104 Stat. 2112, codified in a note to 28 U.S.C. 534.

production equipment and maintenance, production labor, and shipping costs. TSA estimates that the total cost of credentialing production and management will be $17.5 million over five years.

TSA representatives will manage the operation and integration of the TWIC programs, including coordination of a nationwide credentialing rollout program. The Agency will also be responsible for ensuring compliance at all TWIC enrollment facilities. These tasks will require the assignment of permanent TSA personnel and temporary contract labor for program support. Contractors will also certify and accredit TWIC systems on a periodic basis. Support costs will include program travel and office supplies.

TSA has also developed an electronic network (the TSA system) to facilitate applicant information collection, coordination, credential production, applicant notification and the extensive access control activities of all TWIC cardholders and regulated facilities over time. While the majority of the TSA system development costs were financed in prior years with funds appropriated to TSA, system modification costs and recurring operational costs for are included in the five-year program costs.

TSA estimates that the total for program support will be $36.1 million over five years. Table Five details the major cost components TSA expects to incur over the next five years to implement the TWIC program.

Table Five- Year TSA Costs for Transportation Worker Identification Credential Program

Operational Year	Start-Up	1st Year	2nd Year	3rd Year	4th Year	5th
Estimated Annual New Applicants and Turnover	15,000	708,000	164,000	93,000	94,000	
Estimated Annual Lost/Damaged Credential Replacement Applicants	50	27,876	58,003	61,818	62,436	
COST COMPONENTS*						
Threat Assessment Costs						
Personnel to conduct name-based threat assessments	$ 70,000	$ 1,687,000	$ 2,014,000	$ 2,200,000	$ 2,387,000	$
Personnel to conduct redress operations (waivers and appeals)	$ 45,000	$ 537,000	$ 269,000	$ 269,000	$ 269,000	$
Adjudication labor	$ 136,000	$ 3,350,000	$ 1,208,000	$ 824,000	$ 828,000	$
Screening Gateway development	$ 300,000	$ -	$ -	$ -	$ -	$
Screening Gateway operations, maintenance & disaster recovery	$ 247,000	$ 993,000	$ 513,000	$ 513,000	$ 513,000	$
Document management system	$ 42,000	$ 504,000	$ 360,000	$ 240,000	$ 240,000	$
Threat Assessment Costs - Subtotal	$ 840,000	$ 7,071,000	$ 4,364,000	$ 4,046,000	$ 4,237,000	$
Card Production Costs						
Card materials	$ 1,750,000	$ 5,250,000	$ 1,750,000	$ 1,750,000	$ 1,750,000	$
Card production equipment and labor	$ 909,000	$ 1,261,000	$ 937,000	$ 707,000	$ 707,000	$
Production system	$ 250,000	$ -	$ -	$ 100,000	$ -	$

design						
Card re-design	$ -	$ -	$ 100,000	$ -	$ 100,000	$
Shipping	$ 7,000	$ 331,000	$ 100,000	$ 70,000	$ 70,000	$
Card Production Costs - Subtotal	$ 2,916,000	$ 6,842,000	$ 2,887,000	$ 2,627,000	$ 2,627,000	$
Identity Management System (IDMS) Costs						
IDMS labor, O&M, and help desk	$2,850,000	$3,600,000	$1,800,000	$1,680,000	$1,680,000	
IDMS hardware, software, and technology refresh	$188,000	$945,000	$885,000	$825,000	$825,000	
IDMS disaster recovery	$500,000	$100,000	$100,000	$100,000	$100,000	
IDMS Costs - Subtotal	$ 3,538,000	$ 4,645,000	$ 2,785,000	$ 2,605,000	$ 2,605,000	$
Program Support						
Personnel for program support – federal and contract	$ 1,624,000	$ 2,584,000	$ 2,614,000	$ 2,614,000	$ 2,614,000	$
Information systems security certification and accreditation	$ 600,000	$ 250,000	$ 250,000	$ 500,000	$ 250,000	$
Program travel	$ 48,000	$ 144,000	$ 112,000	$ 112,000	$ 112,000	$
Interagency systems and communications infrastructure	$ 481,000	$ 1,085,000	$ 659,000	$ 633,000	$ 630,000	$
Office supplies and miscellaneous program costs	$ 35,000	$ 60,000	$ 60,000	$ 60,000	$ 60,000	$
Fee processing & analysis	$ 17,000	$ 100,000	$ 100,000	$ 100,000	$ 100,000	$

Program Support - Subtotal	$ 2,805,000	$ 4,223,000	$ 3,795,000	$ 4,019,000	$ 3,766,000	$
Enrollment Management and Compliance						
Personnel and operational expenses for enrollment compliance	$ 12,000	$ 584,000	$ 135,000	$ 76,000	$ 77,000	$
Enrollment Management and Compliance - Subtotal	$ 12,000	$ 584,000	$ 135,000	$ 76,000	$ 77,000	$
GRAND TOTALS	$ 10,111,000	$ 23,365,000	$ 13,966,000	$ 13,373,000	$ 13,312,000	$

Threat Assessment/Credential Production Calculation

TSA will charge a fee to recover its threat assessment, credentialing, and other program management and oversight costs associated with the implementation of this rule. TSA notes that since it received appropriated funds for the development of the TWIC program prototype and start-up operations, these costs will not be recovered in the fee charges. Substantially all costs TSA will have incurred before the beginning of program operations are considered start-up costs for calculation of the Threat Assessment/Credential Production fee. Based on the estimated costs in Table Five, TSA has calculated the per applicant Threat Assessment/Credential Production fee as follows: threat assessment cost estimate of $24.1 million over five years is added to credentialing and program expenses of $53.6 million. These total costs are then divided by 1,441,000 total estimated applicants for a TWIC – both new and lost/damaged replacement card applicants – over the first five years.

The resulting applicant charges will range from $50 - $62 per applicant, as fees will vary based on the services provided to each population. Individuals requiring a complete security threat assessment will pay $62. Applicants who have completed a fingerprint-based criminal history records check that TSA deems equivalent to the TWIC check, such as MMD, MML, HME, and FAST credential holders, will not be charged for TSA's adjudication expenses associated with this portion of the threat assessment and will be assessed $50. Individuals who lose, damage, or have their credential stolen will not be assessed any threat assessment costs but will be charged $36 for a replacement credential. No new TSA threat assessment-specific or enrollment costs are factored into this replacement fee.

3. FBI Fee

As part of the security threat assessment, TSA submits fingerprints to the FBI to obtain any criminal history records that correspond to the fingerprints. The FBI is authorized to establish and collect fees to process fingerprint identification records. See Title II of Pub. L. 101-515, November 5, 1990, 104 Stat. 2112, codified in a note to 28 U.S.C. 534. Pursuant to Criminal Justice Information Services (CJIS) Information Letter 93-3 (October 8, 1993), this fee is currently set at $22. If the FBI increases or decreases its fee to complete the criminal history records check, the increase or decrease will apply to this regulation on the date that the new FBI fee becomes effective.

4. Total Fees

TSA proposes the following fees for TWIC applicants who submit fingerprints and applicant information to a TSA agent:

(1)	Information Collection/Credential Issuance	$45 - $65
(2)	Threat Assessment/Credential Production	$50 - $62
(3)	Credential Replacement	$36
(4)	FBI	$22

The total fees for TWIC applicants would be between $95 and $149, depending on threat assessment services provided. TSA will continue to work to minimize all costs and will finalize final fee charges in the final rule. TSA may increase or decrease the fees described in this regulation for inflation following publication of the final rule. TSA will publish a notice in the Federal Register notifying the public of the change.

C. Section 1572.501 Fee Collection.

Section 1572.501 provides that when TSA collects fingerprints and applicant information under 49 CFR part 1572, TSA will collect fees for TWIC, in accordance with the procedures in § 1572.503.

Section 1572.503 describes the procedures that TSA and a TWIC applicant will follow. Paragraph 1572.503(a) list the specific fees: $45 - 65 for information collection/credential issuance; $50 - 62 for the threat assessment/credential production; $36 for a replacement credential; and $22 for the FBI.

Paragraph 1572.503(b) states that the fees must be provided in U.S. currency, and in check, money order, wire, or another method approved by TSA. Paragraph 1572.503(c) states that TSA will not issue refunds and paragraph 1572.503(d) states that applications would be processed only upon receipt of all applicable fees.

Paragraph 1572.503(e) states that TSA may adjust the fees annually after October 1, 2007 because of inflation, and any adjustment will be announced by notice in the Federal Register. Any increase would be a composite of the Federal civilian pay raise percentage and non-pay inflation factor for the current fiscal year. These figures are issued by the Office of Management and Budget.

Paragraph (f) of this section relates to any amendments the FBI may make to its fee for the criminal history records check. The change to the fee for TWIC applicants will become effective on the date that the FBI fee increase or decrease became effective.

VII. Rulemaking Analyses and Notices

A. Executive Order 12866 (Regulatory Planning and Review).

This proposed rule is a "significant regulatory action" under section 3(f) of E.O. 12866, Regulatory Planning and Review and therefore has been reviewed by the

Office of Management and Budget. E.O. 12866 requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. A draft Assessment is available in both the TSA and Coast Guard dockets where indicated under the "Public Participation and Request for Comments" section of this preamble. A summary of the Assessment follows:

Regulatory Evaluation Summary

Proposed changes to Federal regulations must undergo several economic analyses. First, E.O. 12866 directs each Federal agency to propose or adopt a regulation only if the agency makes a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. § 2531-2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. In developing U.S. standards, this Trade Act requires agencies to consider international standards and where appropriate, as the basis of U.S. standards. Fourth, the Unfunded Mandates Reform Act of 1995 (Public Law 104-4) requires agencies to prepare a written assessment of the costs, benefits and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation). The mandatory OMB A-4 Accounting Statement is located in the separate detailed regulatory evaluation.

In conducting these preliminary analyses, TSA and the USCG are proposing that this rule:

1. Is a "significant regulatory action" as defined in the E.O.

2. Has a yet to be determined impact on small business. We have provided an Initial Regulatory Flexibility Analysis (IRFA) for comment.
3. Imposes no significant barriers to international trade.
4. Does not impose an unfunded mandate on State, local, or tribal governments, but does on the private sector as there are two years with undiscounted costs in excess of the inflation adjusted $100 million threshold.

This regulatory evaluation is a joint effort of TSA and USCG. For ease of reading, the agencies decided to use the term "we" to represent both DHS components even for issues which might be directly related to proposed rule actions of only one agency. We believe this simplification will be less of a burden to the public in trying to understand and comment on the evaluation. The reader is cautioned that we did not attempt to replicate precisely the regulatory language in this discussion of the proposed rule; the regulatory text, not the text of this evaluation, is legally binding. A copy of the detailed regulatory evaluation document is available on the dockets for each agency. TSA and the USCG invite comments on all aspects of the economic analysis. We will attempt to evaluate and address all regulatory evaluation comments submitted by the public; however, those comments with specific data sources or detailed information will be more useful in improving the impact analysis. Comments may be placed on either docket as directed in the rule preamble; although there is no prohibition of submitting the evaluation comments to both dockets, duplicate submissions will be treated as a single issue submission. If possible, evaluation comments should be clearly identified with the evaluation issue or section. Including page numbers or figure references with your

comments will expedite the process and insure the issue is addressed by the most appropriate agency experts.

Impact Summary

Section 102 of the Maritime Transportation Security Act requires a regulation regarding the issue of a biometric security card to individuals with unescorted access to secure areas of vessels and facilities. Under this authority, DHS has developed this proposed rule, and this summary provides a synopsis of the costs and benefits of the proposed rule.

Benefits of the Proposed Rule

The proposed rule would facilitate commerce and, most importantly, increase security at vessels, facilities, and OCS facilities regulated by 33 CFR chapter I, subchapter H.

Security

The proposed rule would increase security at vessels, facilities, and OCS facilities regulated by 33 CFR chapter I, subchapter H. It would accomplish this by: (1) reducing the number of high-risk individuals with unescorted access to secure areas of vessels, facilities, and OCS facilities through the use of robust background checks; (2) enhancing the security of the credential through the use of a highly tamper-resistant card and the implementation of a strong identity-verification process to guard against fraud; and (3) increasing the stringency of access control measures throughout the maritime transportation sector.

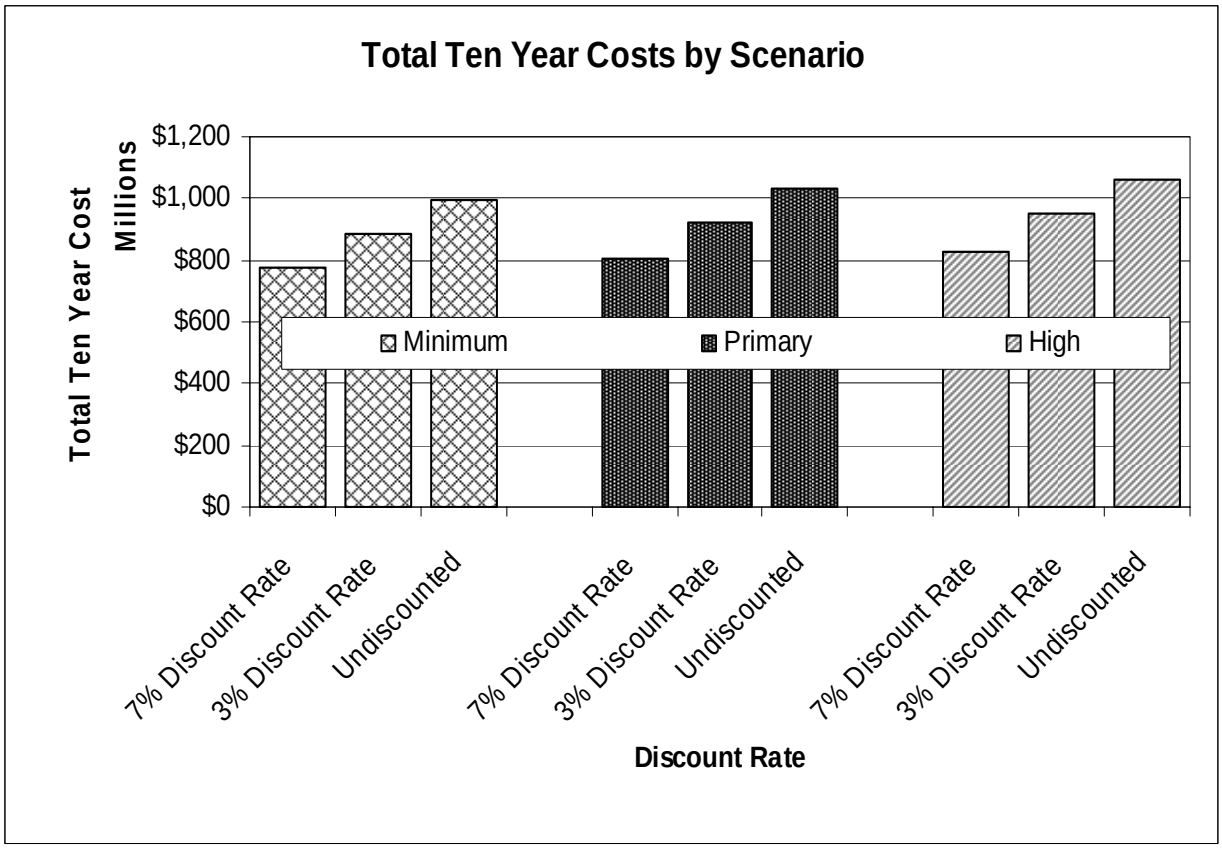
Commerce

Although not the primary impetus for regulation, this NPRM would enhance the flow of commerce by streamlining the number of credentials and access control procedures, eliminating the need for several port credentialing offices and systems, and creating an interoperable credential recognizable across the maritime environment. During the TWIC Phase III Prototype, TSA learned that many individuals underwent multiple background checks, paid redundant fees, and endured long lines and short hours of operation at local credentialing offices. We anticipate this NPRM would eliminate some of these inefficient practices.

Economic Costs

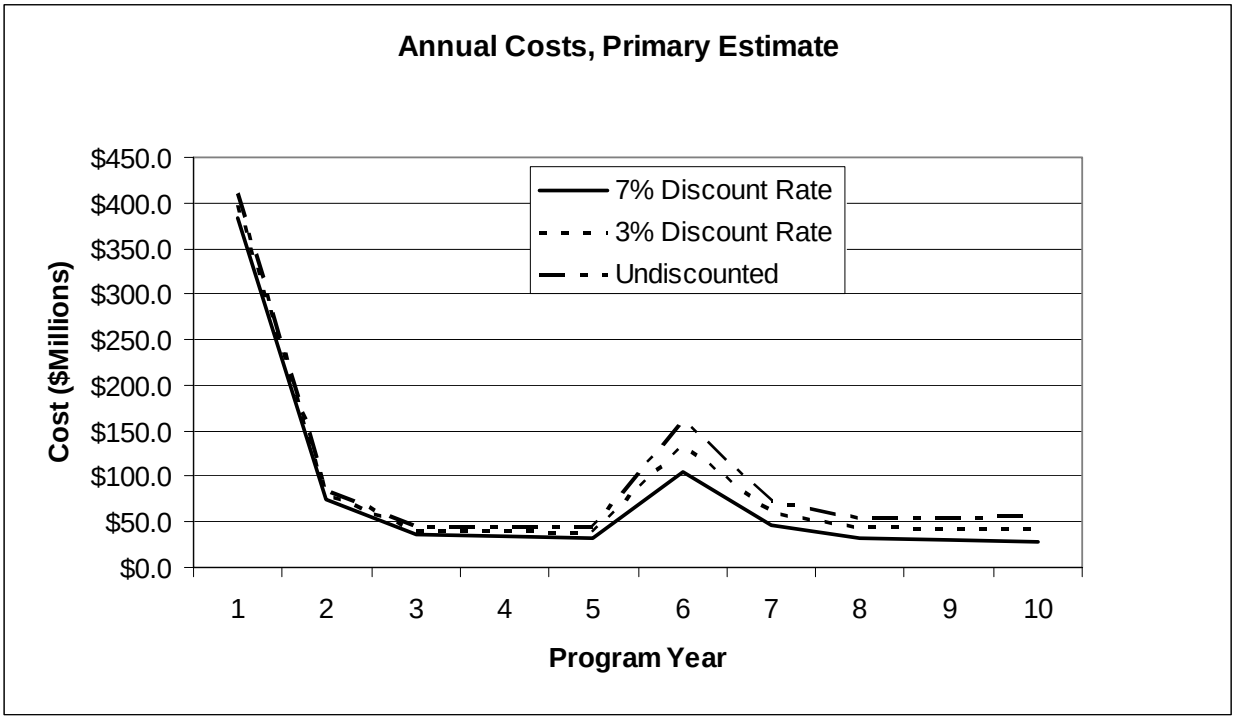
We conclude that the primary estimate of economic costs over a 10 year period for this rule are $1,028 million undiscounted, $918.5 million with a 3 percent discount rate, and $802.8 million at a 7 percent discount rate. In preparing estimates, we considered ranges for some values. No statistical confidence interval is associated with this range. These ranges provide an upper estimate of $1,062 million undiscounted and a lower range of $995.0 million undiscounted. The full list of scenarios and discounted values are displayed in the following charts and figures.

Ten Year Costs		
Minimum	**7% Discount Rate**	**$777,040,010**
	3% Discount Rate	**$888,602,138**
	Undiscounted	**$994,986,264**
Primary	**7% Discount Rate**	**$802,830,101**
	3% Discount Rate	**$918,517,801**
	Undiscounted	**$1,028,754,087**
High	**7% Discount Rate**	**$828,620,192**
	3% Discount Rate	**$948,433,464**
	Undiscounted	**$1,062,521,911**


Total Ten Year Costs by Scenario
Total Ten Year Cost
Millions
$1,200
$1,000
$800
$600
$400
$200
$0
Minimum
Primary
High
7% Discount Rate
3% Discount Rate
Undiscounted
7% Discount Rate
3% Discount Rate
Undiscounted
7% Discount Rate
3% Discount Rate
Undiscounted
Discount Rate

Timing of Costs

The startup costs plus initial enrollments cause roughly 40 percent of expenses to occur in the first program year. Because credentials must be renewed after five years, there is another spike in enrollments and, therefore, expenses at year six. This spike is not as large as the initial enrollment because there is movement in and out of the labor force over those five years. This increase in enrollments in year six represents approximately 15 percent of the total costs. The other eight program years are similar in costs.



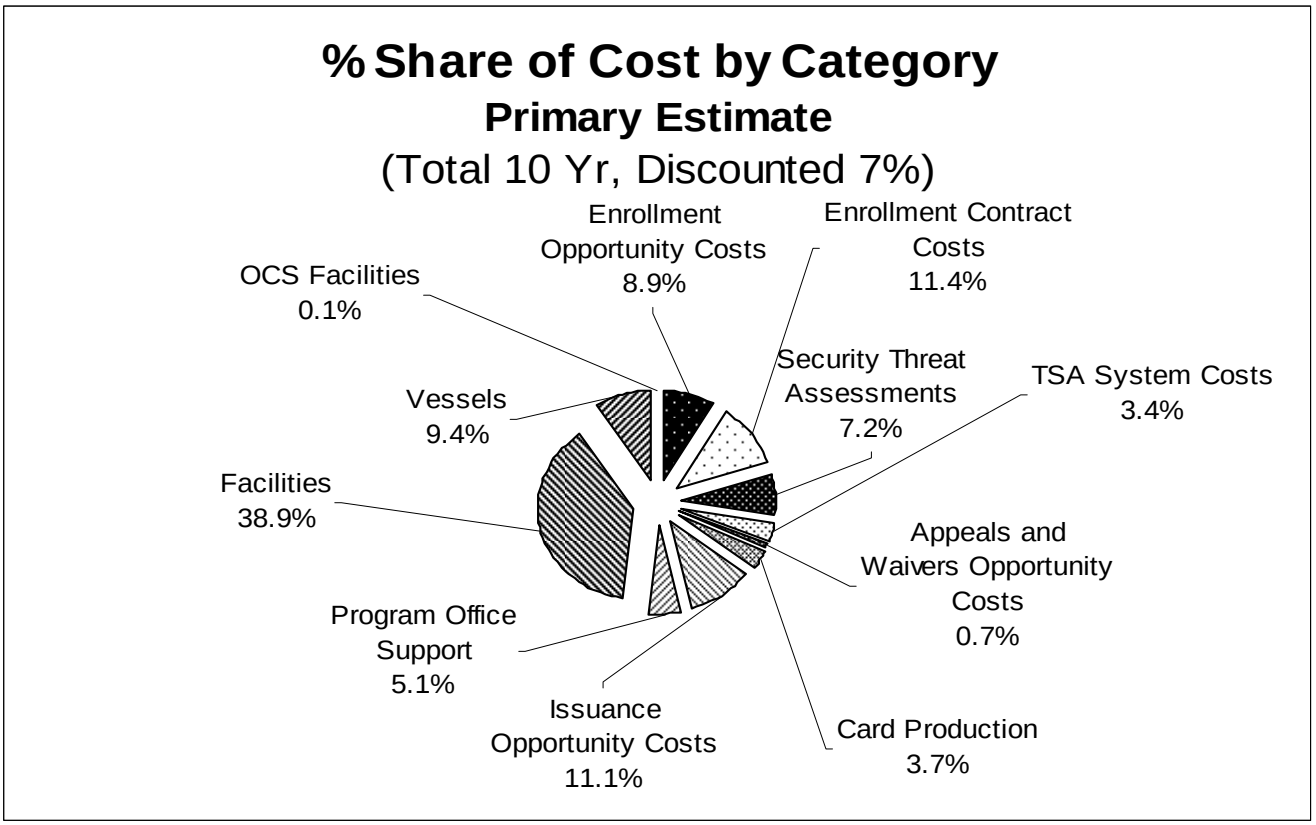
Total Ten-Year Costs -- Primary Estimate ($ millions)											
Discount Rate / Yr	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
7% Discount Rate	**$383.6**	**$74.0**	**$36.7**	**$34.2**	**$32.2**	**$105.7**	**$45.7**	**$32.2**	**$30.1**	**$28.4**	**$802.8**
3% Discount Rate	**$398.5**	**$79.9**	**$41.1**	**$39.8**	**$38.9**	**$132.9**	**$59.7**	**$43.7**	**$42.4**	**$41.6**	**$918.5**

Undiscounted	**$410.4**	**$84.7**	**$44.9**	**$44.8**	**$45.1**	**$158.7**	**$73.4**	**$55.4**	**$55.3**	**$55.9**	**$1,028.8**

Distribution of Costs

The fee setting section of the NPRM and supporting documents in the docket provide details of the distribution of impacts. By category, almost 39 percent of the costs are facility costs, 11 percent enrollment contract costs, while the smallest category of costs is related to Outer Continental Shelf facilities at less than 0.1 percent of the total costs. The following series of figures summarizes the 11 categories for the range of costs discounted at 7 percent, categorical percentage share of total costs, and share differences between the primary estimate and each of the other two scenarios.

Costs by Category and Scenario, Discounted 7%			
Component	**Low**	**Primary**	**High**
Enrollment Opportunity Costs	$71.8	$71.8	$71.8
Enrollment Contract Costs	$91.9	$91.9	$91.9
Security Threat Assessments	$57.9	$57.9	$57.9
TSA System Costs	$27.4	$27.4	$27.4
Appeals and Waivers Opportu	$5.7	$5.7	$5.7
Card Production	$29.5	$29.5	$29.5
Issuance Opportunity Costs	$89.0	$89.0	$89.0
Program Office Support	$41.0	$41.0	$41.0
Facilities	$299.0	$312.1	$325.1
Vessels	$63.1	$75.8	$88.4
OCS Facilities	$0.6	$0.7	$0.8
Total	**$777.0**	**$802.8**	**$828.6**


% Share of Cost by Category
Primary Estimate
(Total 10 Yr, Discounted 7%)
Enrollment Opportunity Costs 8.9%
Enrollment Contract Costs 11.4%
OCS Facilities 0.1%
Security Threat Assessments 7.2%
TSA System Costs 3.4%
Vessels 9.4%
Facilities 38.9%
Appeals and Waivers Opportunity Costs 0.7%
Program Office Support 5.1%
Issuance Opportunity Costs 11.1%
Card Production 3.7%

% Cost Share by Category and Scenario				Difference from Primary Estimate	
Component	**Low**	**Primary**	**High**	**Low**	**High**
Enrollment Opportunity Costs	9.2%	8.9%	8.7%	0.3%	-0.3%
Enrollment Contract Costs	11.8%	11.4%	11.1%	0.4%	-0.4%
Security Threat Assessments	7.5%	7.2%	7.0%	0.2%	-0.2%
TSA System Costs	3.5%	3.4%	3.3%	0.1%	-0.1%
Appeals and Waivers Opportu	0.7%	0.7%	0.7%	0.0%	0.0%
Card Production	3.8%	3.7%	3.6%	0.1%	-0.1%
Issuance Opportunity Costs	11.5%	11.1%	10.7%	0.4%	-0.3%
Program Office Support	5.3%	5.1%	5.0%	0.2%	-0.2%
Facilities	38.5%	38.9%	39.2%	-0.4%	0.4%
Vessels	8.1%	9.4%	10.7%	-1.3%	1.2%
OCS Facilities	0.1%	0.1%	0.1%	0.0%	0.0%
Total	**100.0%**	**100.0%**	**100.0%**	-	-

B. Small Entities

Under the Regulatory Flexibility Act (5 U.S.C. 601-612), we have considered whether this proposed rule would have a significant economic impact on a substantial number of small entities. The term "small entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. Individuals are not considered small entities for the purposes of the Regulatory Flexibility Act.

At this time, we have not determined if this proposed rule would have a significant economic impact on a substantial number of small entities. We request comment on the full Initial Regulatory Flexibility Analysis, which is located on the docket. A brief summary of this analysis appears below.

With certain exceptions, the proposed rule would impact vessels, facilities, and OCS facilities presently regulated by 33 CFR chapter I, subchapter H. TSA and USCG estimated the proposed rule would cover 10,785 vessels, 3,492 facilities, and 42 OCS facilities. TSA and USCG concluded that most vessels and some facilities may be owned

by small businesses, but no small businesses, as defined by the Regulatory Flexibility Act, currently operate OCS facilities.

The proposed rule would require affected vessels, facilities and OCS facilities to implement increased security measures. Because many of the proposed measures are based on performance standards, the proposed rule affords covered businesses flexibility in complying with the requirements. Due to this flexibility, we foresee small entities complying with the proposed rule in a number of ways. We therefore used a range of estimates when characterizing the potential impacts to small entities. The following table displays this range.

Requirement	Initial Costs			Recurring Costs		
	Low	Primary	High	Low	Primary	High
Smart Card Reader Purchase	$2,000	$3,500	$5,000			
Smart Card Reader Software	$1,000	$1,000	$1,000			
Smart Card Reader Installation	$200	$200	$200			
Creating TWIC Addendum	$1,693	$1,691	$1,691			
Knowledge Requirements	$2,709	$2,709	$2,709			
Recordkeeping	$1,303	$1,303	$1,303			
TWIC Validation				$391	$391	$391
Total	**$8,906**	**$10,403**	**$11,903**	**$391**	**$391**	**$391**

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104-121), we want to assist small entities in understanding this proposed rule so that they can better evaluate its effects on them and participate in the rulemaking. If the rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please consult LCDR Jonathan Maiorine, Commandant (G-PCP-2), United States Coast Guard, 2100 Second Street, SW, Washington, DC 20593; telephone 1(877) 687-2243. DHS will

not retaliate against small entities that question or complain about this rule or any policy or action of DHS.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of TSA or of the Coast Guard, call 1-888-REG-FAIR (1-888-734-3247).

D. Collection of Information

This proposed rule would call for a collection of information under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). As defined in 5 CFR 1320.3(c), "collection of information" comprises reporting, recordkeeping, monitoring, posting, labeling, and other, similar actions. The title and description of the information collections, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for reviewing instructions, searching existing sources of data, gathering and maintaining the data needed, and completing and reviewing the collection.

TITLE: Transportation Worker Identification Credential (TWIC) Program.

SUMMARY OF THE COLLECTION OF INFORMATION:

NEED FOR INFORMATION: TSA has developed the Transportation Worker Identification Credential (TWIC) as an identification tool that encompasses the authorities of the Aviation and Transportation Security Act of 2001(ATSA) (Pub. L. 107-71, Sec.106), and

the Maritime Transportation Security Act of 2002 (MTSA) (Pub. L. 107-295, Sec. 102) to perform background checks and issue credentials to workers within the national transportation system. The data to be collected is that biographic and biometric information necessary for TSA to complete the required security threat assessment on individuals who will seek unescorted access to secure areas of vessels and maritime facilities through the use of a TWIC. TWIC cards, when issued, will contain biographic and biometric data necessary to prove identity of the cardholder and to interoperate with access control systems on vessels and at facilities nationwide.

PROPOSED USE OF INFORMATION: TSA will use the information to verify the identity of the individual applying for a TWIC and to verify that the person poses no security threat that would preclude issuance of a TWIC.

DESCRIPTION OF THE RESPONDENTS: The respondents to this collection of information will be workers within the national transportation system, specifically individuals who require unescorted access to secure areas of vessels or maritime facilities.

NUMBER OF RESPONDENTS: Although the number of respondents will vary over three years, TSA estimates that the annualized number of total respondents will be approximately 317,400. Based on research conducted by TSA and the USCG, the total estimated base population that will be affected by TWIC is 750,000. However, TSA estimates that more than seventy percent of the base maritime worker population will enroll in the program in the first year, and the remainder will enroll in year two. Turnover and growth within the affected population is expected to result in another 202,257 respondents.

FREQUENCY OF RESPONSE: Because renewals for the TWIC will be on a five year basis, for purposes of the Paperwork Reduction Act, to apply for a TWIC, each respondent will be required to respond once to the enrollment collection. TSA estimates an additional response from the estimated two percent of respondents who will appeal decisions made by the agency with respect to security threat assessments or ask for a waiver from disqualifying offenses. Thus, TSA estimates the number of total annual responses to be approximately 323,800.

BURDEN OF RESPONSE: TSA estimates the annual hour burden for enrollment to be 476,129, or one and one half hour per respondent. TSA estimates the annual hour burden for appeals and waiver to be approximately 38,100.

TSA has determined that the information collection and card issuance portion of the TWIC fee will be between $45 and $65 per respondent. The exact fee will be determined in the final rulemaking. This portion of the fee accounts for more than the actual cost of the information collection as it includes cost of the enrollment process, system operations and maintenance, and TWIC card distribution.

ESTIMATE OF TOTAL ANNUAL BURDEN: TSA estimates the total annual hour burden as a result of this collection of information to be approximately 514,200. Because the TWIC fee may change over time as actual costs are determined and annualized, TSA estimates total annual fee for respondents to be between $14,283,855 and $20,632,235.

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), we have submitted a copy of this proposed rule to the Office of Management and Budget (OMB) for its review of the collection of information.

We ask for public comment on the proposed collection of information to help us determine how useful the information is; whether it can help us perform our functions better; whether it is readily available elsewhere; how accurate our estimate of the burden of collection is; how valid our methods for determining burden are; how we can improve the quality, usefulness, and clarity of the information; and how we can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under ADDRESSES, by the date under DATES.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. Before the requirements for this collection of information become effective, we will publish notice in the Federal Register of OMB's decision to approve, modify, or disapprove the collection.

E. Federalism

A rule has implications for federalism under E.O. 13132, Federalism, if it has a substantial direct effect on State or local governments and would either preempt State law or impose a substantial direct cost of compliance on them. TSA and Coast Guard have analyzed this proposed rule under that Order and have determined that it has implications for federalism, for the same reasons that we found Federalism impacts for the Coast Guard's previously published MTSA regulations. 68 FR at 60468-9. A summary of the impacts on federalism in this proposed rule follows.

This proposed rule would have a substantial direct effect on States, local governments, or political subdivisions under section 1(a) of the Order when those states

owning vessels/facilities are required to submit a TWIC Addendum and implement a TWIC program. It would also preempt State law under section 6(c) of the Order by: continuing to prevent States from regulating mariners; and continuing to prevent the States from requiring security plans. It would impose substantial direct costs of compliance on States or local governments under section 6(b) of the Order, by requiring the submission of a TWIC Addendum and the implementation of TWIC on State owned vessels or facilities.

Regulations already issued by the Coast Guard under other sections of the MTSA of 2002 cited the need for national standards of security, claimed preemption, and received comments in support of such a scheme. See 68 FR 60448, 60468-60469. (October 23, 2003).

The law is well-settled that States may not regulate in categories expressly reserved for regulation by the Coast Guard. The law also is well-settled that all of the categories covered in 46 U.S.C. 3306, 3703, 7101, and 8101 (design, construction, alteration, repair, maintenance, operation, equipping, personnel qualification, and manning of vessels), as well as the reporting of casualties and any other category in which Congress intended the Coast Guard to be the sole source of a vessel's obligations, are within the field foreclosed from regulation by the States. See United States v. Locke and Intertanko v. Locke, 529 U.S. 89, 120 S.Ct. 1135 (Mar. 6, 2000). Since portions of this proposed rule involve the manning of U.S. vessels and the licensing of merchant mariners, it relates to personnel qualifications. Because the states may not regulate within this category, these portions of this proposed rule do not present new preemption issues under E.O. 13132.

We are only asserting field preemption in those areas where federal regulations have historically dominated the field, such as merchant mariner regulations, or where we are amending regulations that we have previously asserted preempt state regulation, such as the Marine Transportation Security Act Regulations found in 33 CFR chapter I, subchapter H. States would not be preempted from instituting their own background checks or badging systems in addition to the TWIC.

We are asking for comments specifically on the issue of preemption.

F. Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular, the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100,000,000 or more in any one year. This proposed rule would result in such an expenditure, and we discuss the effects of this rule in the Draft Regulatory Evaluation, which is summarized in the E.O. 12866 section above.

G. Taking of Private Property

This proposed rule would not affect a taking of private property or otherwise have taking implications under E.O. 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights.

H. Civil Justice Reform

This proposed rule meets applicable standards in sections 3(a) and 3(b)(2) of E.O. 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden.

I. Protection of Children

We have analyzed this proposed rule under E.O. 13045, Protection of Children from Environmental Health Risks and Safety Risks. While this rule is an economically significant rule, it would not create an environmental risk to health or risk to safety that might disproportionately affect children.

J. Indian Tribal Governments

This proposed rule does not have tribal implications under E.O. 13175, Consultation and Coordination with Indian Tribal Governments, because it would not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

K. Energy Effects

We have analyzed this proposed rule under E.O. 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use. We have determined that it is not a "significant energy action" under that order. While it is a "significant regulatory action" under E.O. 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy. The Administrator of the Office of Information and Regulatory Affairs has not designated it as a significant energy action. Therefore, a Statement of Energy Effects is not required for this rule under E.O. 13211.

L. Technical Standards

The National Technology Transfer and Advancement Act (NTTAA) (15 U.S.C. 272 note) directs agencies to use voluntary consensus standards in their regulatory

activities unless the agency provides Congress, through the Office of Management and Budget, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (e.g., specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies.

This rulemaking will incorporate standards for TWIC readers and card technology. These standards have been developed by the Federal government; there are no voluntary consensus standards that could be used in their place.

M. Environment

This Transportation Worker Identification Credential (TWIC) proposal contains a program of activities to improve the safety and security of vessels, facilities, Outer Continental Shelf facilities, and U.S. ports. It proposes requirements for developing application forms, collecting and processing forms, application evaluation criteria, and issuing determinations on applications. It also updates the training, qualifying, licensing, and disciplining of maritime personnel and proposes amendments to security plans that will contribute to a higher level of marine safety and security for vessels, facilities, Outer Continental Shelf facilities, and U.S. ports.

Implementation of this proposal will involve establishing "enrollment stations" inside existing port facilities to collect TWIC applications. The enrollment stations will include a small office, using existing utilities, located in space made available in existing port facilities or other available space within a 25 mile radius of the port facility. If a location does not have a port facility, or enough space, a temporary unit will be provided

until either sufficient permanent space is available or the need for the enrollment station no longer exists. To meet the initial surge of enrollments expected when the rule is final, 138 stations (permanent and mobile/temporary) are expected to be operating nationwide. The on-going/maintenance phase will involve approximately 134 stations.

The provisions of this proposed rule have been analyzed under the Department of Homeland Security (DHS) Management Directive (MD) 5100.1, Environmental Planning Program, which is the DHS policy and procedures for implementing the National Environmental Policy Act (NEPA), and related E.O.s and requirements. The implementation of this rule is expected to be categorically excluded under the following categorical exclusions (CATEX) listed in MD 5100.1, Appendix A, Table 1: CATEX A1 (personnel, fiscal, management and administrative activities); CATEX A3 (promulgation of rules, issuance of rulings or interpretations); and CATEX A4 (information gathering, data analysis and processing, information dissemination, review, interpretation and development of documents). CATEX B3 (proposed activities and operations conducted in an existing structure that would be compatible with and similar in scope to ongoing functional uses) is also applicable. Additionally, we have determined that there are no extraordinary circumstances presented by this rule that would limit the use of a CATEX under MD 5100.1, Appendix A, paragraph 3.2.

VIII. List of Subjects

33 CFR Part 101

Harbors, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

33 CFR Part 103

Facilities, Harbors, Maritime security, Ports, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

33 CFR Part 104

Incorporation by reference, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels.

33 CFR Part 105

Facilities, Maritime security, Reporting and recordkeeping requirements, Security measures.

33 CFR Part 106

Facilities, Maritime security, Outer Continental Shelf, Reporting and recordkeeping requirements, Security measures.

33 CFR Part 125

Administrative practice and procedure, Harbors, Reporting and recordkeeping requirements, Security measures, Vessels.

46 CFR Part 10

Penalties, Reporting and recordkeeping requirements, Schools, Seamen.

46 CFR Part 12

Penalties, Reporting and recordkeeping requirements, Seamen.

46 CFR Part 15

Reporting and recordkeeping requirements, Seamen, Vessels.

49 CFR Part 1515

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime

security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

49 CFR Part 1570

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

49 CFR Part 1572

Appeals, Commercial drivers license, Criminal history background checks, Explosives, Facilities, Hazardous materials, Incorporation by reference, Maritime security, Motor carriers, Motor vehicle carriers, Ports, Seamen, Security measures, Security threat assessment, Vessels, Waivers.

IX. The Amendments

For the reasons listed in the preamble, the Coast Guard proposes to amend 33 CFR parts 101, 103, 104, 105, 106, 125; and 46 CFR parts 10, 12, and 15 and the Transportation Security Administration proposes to add or amend 49 CFR parts 1515, 1570, and 1572 as follows:

33 CFR PART 101—MARITIME SECURITY: GENERAL

1. The authority citation for part 101 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.1.

2. In § 101.105 add, in alphabetical order, definitions for the terms escorting, personal identification number (PIN), recurring unescorted access, secure area, TWIC, TWIC program, and unescorted access, to read as follows:

§ 101.105 Definitions.

* * * * *

Escorting means ensuring that the escorted individual is continuously accompanied or monitored while within a secure area in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted.

* * * * *

Personal Identification Number (PIN) means a personally selected number stored electronically on the individual's TWIC.

* * * * *

Recurring unescorted access means authorization to enter a vessel on a continual basis after an initial personal identity and credential verification, as outlined in the vessel security plan.

* * * * *

Secure Area means the area on board a vessel or at a facility or outer continental shelf facility over which the owner/operator has implemented security measures for access control, as defined by a Coast Guard approved security plan. It does not include passenger access areas or public access areas, as those terms are defined in sections 104.106 and 105.106 of this subchapter.

* * * * *

TWIC means a valid, non-revoked transportation worker identification credential, as defined and explained in 49 CFR part 1572.

TWIC Program means those procedures and systems, detailed in an approved security plan, that a vessel, facility, or outer continental shelf facility must implement in order to assess and validate TWICs when maintaining access control.

* * * * *

Unescorted access means having the authority to enter and move about a secure area without escort.

* * * * *

3. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], add § 101.121 to read as follows:

§ 101.121 Alternative Security Programs – TWIC Addendum.

(a) Submitters of Alternative Security Programs that have been approved by the Commandant (G-PC) under section 101.120 of this part, must submit a TWIC Addendum by [insert date six months after date of publication of final rule], or else their Alternative Security Plan is invalid. The TWIC Addendum should include an explanation of how the ASP addresses the requirements for a TWIC program contained in parts 104, 105 and 106 of this subchapter, as applicable.

(b) The Commandant (G-PC) will examine each TWIC Addendum for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its approval and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(c) The ASP TWIC Addendum will be given the same expiration date as the ASP.

(d) Upon gaining approval of the TWIC Addendum, the submitter of the ASP must incorporate the approved TWIC Addendum into their ASP when it is due for reapproval in accordance with section 101.120 of this subpart.

4. Add § 101.514 to read as follows:

§ 101.514 TWIC Requirement.

(a) All persons requiring unescorted access to secure areas of vessels, facilities, and OCS facilities regulated by parts 104, 105 or 106 of this subchapter must possess a TWIC before such access is granted, except as otherwise noted in this section. A TWIC must be obtained via the procedures established by TSA in 49 CFR part 1572.

(b) Federal officials are not required to obtain or possess a TWIC. Except in cases of emergencies or other exigent circumstances, in order to gain unescorted access to a secure area of a vessel, facility, or OCS facility regulated by parts 104, 105 or 106 of this subchapter, he/she must verify his identity at a TWIC reader using his/her agency issued, HSPD 12 compliant, credential. Until each agency issues its HSPD 12 compliant cards, Federal officials may gain unescorted access by using their agency's official credential. The COTP will advise facilities and vessels within his area of responsibility as agencies come into compliance with HSPD 12.

(c) Law enforcement officials at the State or local level are not required to obtain or possess a TWIC to gain unescorted access to secure areas. They may, however, voluntarily obtain a TWIC where their offices fall within or where they desire recurring unescorted access to a secure area of a vessel, facility or OCS facility.

(d) Owners and/or operators of any vessel or maritime facility that is not required to comply with parts 104, 105, or 106 of this subchapter, respectively, who would like to implement a TWIC Program for their vessel or facility must contact their cognizant COTP to gain authorization. If approved, the Coast Guard will contact TSA, who will provide the authorization to enroll the vessel or facility employees at a TWIC enrollment center.

5. Revise § 101.515 read as follows:

§ 101.515 TWIC/Personal Identification.

(a) Persons not described in section 101.514 of this part shall be required to present personal identification in order to gain entry to a vessel, facility, and OCS facility regulated by parts 104, 105 or 106 of this subchapter. These individuals must be escorted at all times while in a secure area. This personal identification must, at a minimum, meet the following requirements:

(1) Be laminated or otherwise secure against tampering;

(2) Contain the individual's full name (full first and last names, middle initial is acceptable);

(3) Contain a photo that accurately depicts that individual's current facial appearance; and

(4) Bear the name of the issuing authority.

(b) The issuing authority in paragraph (b)(4) of this section must be:

(1) A government authority, or an organization authorized to act of behalf of a government authority; or

(2) The individual's employer, union, or trade association.

(c) Vessel, facility, and OCS facility owners and operators must permit law enforcement officials, in the performance of their official duties, who present proper identification in accordance with this section and § 101.514 of this part to enter or board that vessel, facility, or OCS facility at any time, without delay or obstruction. Law enforcement officials, upon entering or boarding a vessel, facility, or OCS facility, will, as soon as practicable, explain their mission to the Master, owner, or operator, or their designated agent.

33 CFR Part 103—MARITIME SECURITY: AREA MARITIME SECURITY

6. The authority citation for part 103 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70102, 70103, 70104, 70112; 50 U.S.C. 191; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

7. Amend § 103.305(c) to read as follows:

§ 103.305 Composition of an Area Maritime Security (AMS) Committee.

* * * * *

(c) Members appointed under this section serve for a term of not more than 5 years. In appointing members, the FMSC should consider the skills required by § 103.410 of this part. With the exception of credentialed Federal, state and local officials,

all AMS Committee members shall hold a TWIC, or have passed a comparable security threat assessment, as determined by the FMSC.

8. In § 103.505, amend paragraph (n) to read as follows:

§ 103.505 Elements of the Area Maritime Security (AMS) plan.

* * * * *

(n) Security measures designed to ensure the effective security of infrastructure, special events, vessels, passengers, cargo, and cargo handling equipment at facilities within the port not otherwise covered by a Vessel or Security Plan, approved under part 104, 105, or 106 of this subchapter. This includes the use of a TWIC program.

* * * * *

9. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], in § 103.510, designate the existing text as paragraph (a) and add paragraph (b) to read as follows:

§ 103.510 Area Maritime Security (AMS) Plan review and approval.

* * * * *

(b) Each AMS Plan shall be updated to include the implementation of the TWIC program.

33 CFR Part 104—MARITIME SECURITY: VESSELS

10. The authority citation for part 104 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

11. Amend § 104.105 by redesignating paragraph (d) as paragraph (e) and adding a new paragraph (d) to read as follows:

§ 104.105 Applicability.

* * * * *

(d) The TWIC requirements found in this part do not apply to foreign vessels.

* * * * *

12. Add § 104.106 to read as follows:

§ 104.106 Passenger Access Area.

(a) A ferry, passenger vessel, or cruise ship may designate areas within the vessel as passenger access areas. Any such areas must be specified in the VSP.

(b) A passenger access area is a defined space within the access control area of a ferry or passenger vessel that is open to passengers. It is not a secure area and does not require a TWIC for unescorted access.

13. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], amend § 104.115 by adding paragraph (d) to read as follows:

§ 104.115 Compliance dates.

* * * * *

(d) Vessel owners or operators subject to paragraph (b) of this section and not excluded by 104.105(d) or this part must:

(1) Submit a TWIC Addendum to the Commanding Officer, Marine Safety Center, to cover each vessel they own or operate subject to this part on or before [insert date 6 months after publication of the final rule]; and

(2) Be operating in accordance with the TWIC provisions found within this part, as outlined in their TWIC Addendum, between [insert date 1 year after publication of the final rule] and [insert date 18 months after publication of the final rule], depending on whether enrollment has been completed in the port in which the vessel is operating, in accordance with 49 CFR 1572.19.

14. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], amend § 104.120 by adding paragraph (c) to read as follows:

§ 104.120 Compliance documentation.

* * * * *

(c) Each vessel owner or operator subject to this part must ensure, before [insert date one year after publication of the final rule] that copies of the following documentation are carried on board the vessel and are made available to the Coast Guard upon request:

(1) The approved TWIC addendum and any approved revisions or amendments thereto, and a letter of approval from the Commanding Officer, Marine Safety Center (MSC) dated within the last 5 years;

(2) The TWIC Addendum submitted for approval and current written acknowledgment from the Commanding Officer, MSC, stating that the Coast Guard is currently reviewing the TWIC Addendum submitted for approval and that the vessel may continue to operate; or

(3) For vessels operating under a Coast Guard-approved Alternative Security Program as provided in §104.140, a copy of the Alternative Security Program the vessel is using, including a vessel specific security assessment report generated under the

Alternative Security Program, as specified in §101.120(b)(3) of this subchapter, and a letter signed by the vessel owner or operator, stating which Alternative Security Program the vessel is using and certifying that the vessel is in full compliance with that program, as it has been amended pursuant to §101.121 of this subchapter.

Subpart B—Vessel Security Requirements

15. Revise § 104.200(b) to read as follows:

§ 104.200 Owner or operator.

* * * * *

(b) For each vessel, the vessel owner or operator must:

(1) Define the security organizational structure for each vessel and provide all personnel exercising security duties or responsibilities within that structure with the support needed to fulfill security obligations;

(2) Designate, in writing, by name or title, a Company Security Officer (CSO), a Vessel Security Officer (VSO) for each vessel, and identify how those officers can be contacted at any time;

(3) Ensure personnel receive training, drills, and exercises enabling them to perform their assigned security duties;

(4) Inform vessel personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(5) Ensure vessel security records are kept;

(6) Ensure that adequate coordination of security issues takes place between vessels and facilities; this includes the execution of a Declaration of Security (DoS);

(7) Ensure coordination of shore leave, transit, or crew change-out for vessel personnel, as well as access through the facility of visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with facility operators in advance of a vessel's arrival. Vessel owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations in coordinating such leave. The text of these treaties can be found at http://www.marad.dot.gov/Programs/treaties.html;

(8) Ensure security communication is readily available;

(9) Ensure coordination with and implementation of changes in Maritime Security (MARSEC) Level;

(10) Ensure that security systems and equipment are installed and maintained, including at least one TWIC reader that meets the standard incorporated by TSA at 49 CFR 1572.23, and that computer and access control systems and hardware are secure;

(11) Ensure that vessel access, including the embarkation of persons and their effects, are controlled;

(12) Ensure that TWIC procedures are implemented as set forth in this part, including;

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in secure areas in accordance with the VSP are permitted to escort; and

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted.

(13) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(14) Ensure that protocols are in place for responding to TWIC holders presenting for entry who cannot electronically verify a match between themselves and the information stored on the credential's ICC. These must include interim alternative security measures for an individual who cannot electronically verify his identity. Such provisions should take into account measures appropriate for occasional failures to verify and for persistent problems with verification such that a person may require a new credential;

(15) Ensure that protocols are in place for responding to TWIC holders presenting for entry whose cards have been revoked by TSA, and provisions for individuals requiring access who report a lost or stolen TWIC;

(16) Ensure there are alternate provisions in case of equipment or power failures that affect TWIC readers and other validation equipment.

(17) Ensure that appropriate personnel know who is on the vessel at all times;

(18) Ensure that cargo and vessel stores and bunkers are handled in compliance with this part;

(19) Ensure restricted areas, deck areas, and areas surrounding the vessel are monitored;

(20) Provide the Master, or for vessels on domestic routes only, the CSO, with the following information:

(i) Parties responsible for appointing vessel personnel, such as vessel management companies, manning agents, contractors, concessionaires (for example, retail sales outlets, casinos, etc.);

(ii) Parties responsible for deciding the employment of the vessel, including time or bareboat charters or any other entity acting in such capacity; and

(iii) In cases when the vessel is employed under the terms of a charter party, the contract details of those documents, including time or voyage charters; and

(21) Give particular consideration to the convenience, comfort, and personal privacy of vessel personnel and their ability to maintain their effectiveness over long periods.

16. Revise § 104.210 by adding paragraphs (a)(5), (b)(2)(xv) and (c)(15) to read as follows:

§ 104.210 Company Security Officer (CSO).

(a) * * *

(5) The CSO must maintain a valid TWIC.

(b) * * *

(2) * * *

(xv) Knowledge of TWIC

(c) * * *

(15) Ensure the TWIC program is being properly implemented.

17. Revise § 104.215 by adding paragraphs (a)(6), (b)(7) and (c)(12) to read as follows:

§ 104.215 Vessel Security Officer (VSO).

(a) * * *

(6) The VSO must maintain a valid TWIC.

(b) * * *

(7) TWIC

(c) * * *

(12) Ensure TWIC programs are in place and implemented appropriately.

18. Revise § 104.220 by amending the introductory paragraph and adding paragraph (n) to read as follows:

§ 104.220 Company or vessel personnel with security duties.

Company and vessel personnel responsible for security duties must maintain a valid TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(n) Relevant aspects of the TWIC program and how to carry them out.

19. Revise § 104.225 by adding paragraph (f) to read as follows:

§ 104.225 Security training for all other personnel.

* * * * *

(f) Relevant aspects of the TWIC program and how to carry them out.

20. Revise § 104.235 by renumbering paragraphs (b)(1) through (b)(8) as (b)(2) through (b)(9), respectively, and add new paragraph (b)(1) to read as follows:

§ 104.235 Vessel recordkeeping requirements.

* * * * *

(b) * * *

(1) Access. Records of those individuals who are granted access to secure areas of the vessel, including records of when these individuals disembark the vessel and, in the case of individuals who are escorted, the identification of the individual who escorted or the method by which the individual was escorted;

* * * * *

21. Revise § 104.265 to read as follows:

§ 104.265 Security measures for access control.

(a) General. The vessel owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on board;

(3) Control access to the vessel; and

(4) Prevent an unescorted individual from entering an area of the vessel that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area in accordance with the vessel security plan.

(b) The vessel owner or operator must ensure that the following are specified:

(1) The locations providing means of access to the vessel where access restrictions or prohibitions are applied for each Maritime Security (MARSEC) Level,

including those points where a TWIC reader is or will be deployed. “Means of access” include, but are not limited, to all:

(i) Access ladders;

(ii) Access gangways;

(iii) Access ramps;

(iv) Access doors, side scuttles, windows, and ports;

(v) Mooring lines and anchor chains; and

(vi) Cranes and hoisting gear;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and procedures for escorting, in accordance with 101.515; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The vessel owner or operator must ensure that a TWIC program is implemented as follows:

(1) Determine whether recurring unescorted access will be used and, prior to granting any individual recurring unescorted access (as defined in section 101.105 of this subchapter) to secure areas of the vessel, ensure that the individual being granted recurring access privileges has a TWIC and verify the individual’s identity. The identity verification procedure must electronically verify a match between the individual and the biometric information stored on the TWIC’s ICC, including a verification of the

individual's personal identification number (PIN). The validity of the TWIC itself shall also be verified at this time;

(2) After granting recurring unescorted access, verify the individual's identity at each entry to the secure area of the vessel. This identity verification procedure must be outlined in the approved VSP and should at a minimum include visual facial recognition;

(3) Ensure that any individual granted unescorted access to secure areas of the vessel is able to produce his or her TWIC upon request;

(4) Ensure that the identity of any individual not granted recurring unescorted access and seeking unescorted access to the vessel is verified by matching the individual to the biometric information stored on the TWIC's ICC at every entry. The validity of the TWIC itself shall also be verified at this time;

(5) Includes disciplinary measures to prevent fraud and abuse;

(6) Allows certain long-term, frequent vendor representatives and visitors, including seafarers' chaplains and union representatives who hold a TWIC to be eligible for recurring unescorted access;

(7) Allows for temporary access if alternative security measures are implemented due to a failure of the TWIC system, and the individual can meet or pass those alternative security measures;

(8) Is coordinated, when practicable, with identification and TWIC systems at facilities used by the vessel; and

(9) Periodically verifies the validity of TWICs as outlined in paragraphs (f)(1), (g)(1) and (h)(1) of this section.

(d) If the vessel owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The vessel owner or operator must establish in the approved Vessel Security Plan (VSP) the frequency of application of any security measures for access control, particularly if these security measures are applied on a random or occasional basis.

(f) MARSEC Level 1. The vessel owner or operator must ensure security measures in this paragraph are implemented to:

(1) Employ TWIC as set out in paragraph (c) of this section. The validity of a TWIC presented for unescorted access shall be verified using information that is no more than seven (7) days old. The validity of a TWIC held by a person previously granted recurring unescorted access shall be verified weekly, using the most current information available from TSA.

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles for dangerous substances and devices at the rate specified in the approved Vessel Security Plan (VSP), except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Boarding the vessel is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to board;

(4) Check the identification of any person not holding a TWIC and seeking to board the vessel, including vessel passengers, vendors, personnel duly authorized by the

cognizant government authorities, and visitors. This check includes confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of vessel personnel, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the vessel;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which passengers and visitors have access;

(9) Provide a designated area on board, within the secure area, or in liaison with a facility, for conducting inspections and screening of people, baggage (including carry-on items), personal effects, vehicles and the vehicle's contents;

(10) Ensure vessel personnel are not subjected to screening, of the person or of personal effects, by other vessel personnel, unless security clearly requires it. Any such

screening must be conducted in a way that takes into full account individual human rights and preserves the individual's basic human dignity;

(11) Ensure the screening of all unaccompanied baggage;

(12) Ensure checked persons and their personal effects are segregated from unchecked persons and their personal effects;

(13) Ensure embarking passengers are segregated from disembarking passengers;

(14) Ensure, in liaison with the facility, a defined percentage of vehicles to be loaded aboard passenger vessels are screened prior to loading at the rate specified in the approved VSP;

(15) Ensure, in liaison with the facility, all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading; and

(16) Respond to the presence of unauthorized persons on board, including repelling unauthorized boarders.

(g) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the vessel owner or operator must:

(1) Verify the validity of a TWIC presented for unescorted access using information that is no more than one (1)_day old, and verify the validity of TWIC credentials presented by persons granted recurring unescorted access to the vessel daily, using the most current information available from TSA; and

(2) Ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved VSP. These additional security measures may include:

(i) Increasing the frequency and detail of screening of people, personal effects, and vehicles being embarked or loaded onto the vessel as specified for MARSEC Level 2

in the approved VSP, except for government-owned vehicles on official business when government personnel present identification credentials for entry;

(ii) X-ray screening of all unaccompanied baggage;

(iii) Assigning additional personnel to patrol deck areas during periods of reduced vessel operations to deter unauthorized access;

(iv) Limiting the number of access points to the vessel by closing and securing some access points;

(v) Denying access to visitors who do not have a verified destination;

(vi) Deterring waterside access to the vessel, which may include, in liaison with the facility, providing boat patrols; and

(vii) Establishing a restricted area on the shore side of the vessel, in close cooperation with the facility.

(h) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, the vessel owner or operator must:

(1) Require all persons, including those granted recurring unescorted access to secure areas of the vessel in accordance with paragraph (c)(1), to verify their identity at each entry to a secure area by electronically matching the individual to the biometric information stored on the TWIC, including a verification of the individual's PIN;

(2) Ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved VSP. The additional security measures may include:

(i) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(ii) Performing one or more of the following on unaccompanied baggage:

(A)_Screen unaccompanied baggage more extensively, for example, x-raying from two or more angles;

(B) Prepare to restrict or suspend handling unaccompanied baggage; or

(C) Refuse to accept unaccompanied baggage on board;

(iii) Being prepared to cooperate with responders and facilities;

(iv) Limiting access to the vessel to a single, controlled access point;

(v) Granting access to only those responding to the security incident or threat thereof;

(vi) Suspending embarkation and/or disembarkation of personnel;

(vii) Suspending cargo operations;

(viii) Evacuating the vessel;

(ix) Moving the vessel; or

(x) Preparing for a full or partial search of the vessel

22. Revise § 104.290 by redesignating paragraphs (a)(1) through (a)(5) as (a)(2) through (a)(6), respectively, and adding new paragraph (a)(1) to read as follows:

§ 104.290 Security incident procedures.

* * * * *

(a) * * *

(1) Providing a list of all individuals who have been granted access to the vessel, as maintained pursuant to § 104.235 of this part;

* * * * *

23. Revise § 104.295 to read as follows:

§ 104.295 Additional requirements—cruise ships.

(a) The owner or operator of a U.S.-flagged cruise ship must ensure the following:

(1) At all MARSEC levels:

(i) Each crewmember or employee's identity and TWIC must be verified prior to allowing the individual to board the vessel at each entry to the vessel. The TWIC validation procedure must rely upon the most current information available from TSA. The identity verification procedure must electronically verify a match between the individual and the biometric information stored on the TWIC's ICC.

(ii) All persons, baggage, and personal effects must be screened for dangerous substances and devices;

(iii) The identification of all persons seeking to board the vessel must be checked. Persons holding a TWIC shall be checked as set forth in paragraph (a)(1) of this section. For persons not holding a TWIC, this check includes confirming the reason for boarding by examining passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(iv) Security patrols must be performed; and

(v) Selected areas must be searched prior to embarking passengers and prior to sailing.

(2) At MARSEC Level 2, in addition to the requirements of paragraph (a)(1)(i), above the owner or operator of a U.S.-flagged cruise ship must ensure that each crewmember or employee seeking to board the vessel is required to enter his or her correct PIN prior to being allowed to board.

(3) At MARSEC Level 3, the owner or operator of a U.S.-flagged cruise ship must ensure that security briefs to passengers about the specific threat are provided.

(b) The owner or operator of a foreign-flagged cruise ship must ensure the following:

(1) At all MARSEC Levels:

(i) All persons, baggage, and personal effects must be screened for dangerous substances and devices;

(ii) The identification of all persons seeking to board the vessel must be checked, and must include confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(iii) Perform security patrols; and

(iv) Search selected areas prior to embarking passengers and prior to sailing.

(2) At MARSEC Level 3, the owner or operator of a foreign cruise ship must ensure that security briefs to passengers about the specific threat are provided.

Subpart D—Vessel Security Plan (VSP)

24. Revise § 104.405(a)(10) to read as follows:

§ 104.405 Format of the Vessel Security Plan (VSP).

(a) * * *

(10) Security measures for access control, including designated passenger access areas and TWIC implementation;

* * * * *

25. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], add Subpart E—TWIC Addendum to read as follows:

Subpart E—TWIC Addendum

104.500 General.

104.505 Submission and approval.

104.510 Integration of TWIC Addendum into full VSP.

§ 104.500 General.

A vessel owner or operator must ensure the completion of a TWIC Addendum. The TWIC Addendum must outline the security measures to be used on the vessel in order to implement a TWIC program as discussed in section 104.265 of this part, including the alternate procedures to be used.

§ 104.505 Submission and approval.

(a) In accordance with § 104.115, on or before [insert date six months after publication of the final rule], each vessel owner or operator not operating under an ASP must submit one copy of their TWIC Addendum, in English, for review and approval to the Commanding Officer, Marine Safety Center (MSC) and a letter certifying that their TWIC Addendum meets applicable requirements of this part.

(b) Owners or operators of vessels not in service on or before [insert date of publication of final rule] must comply with section 104.510 and submit a complete VSP that includes details regarding the implementation of a TWIC program.

(c) The Commanding Officer, MSC, will examine each submission for compliance with this subpart and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a letter to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a letter to the submitter with a brief statement of the reasons for disapproval.

(d) A TWIC Addendum may be submitted and approved to cover more than one vessel where the vessel design and operations are similar.

(e) Each company or vessel owner or operator that submits one TWIC Addendum to cover two or more vessels of similar design and operation must address vessel-specific information that includes the physical and operational characteristics of each vessel.

(f) A TWIC Addendum will be given the same expiration date as the vessel's full VSP.

§ 104.510 Integration of TWIC Addendum into full VSP.

Upon gaining approval for the TWIC Addendum, the vessel owner or operator must incorporate the approved TWIC Addendum into the VSP when the vessel's VSP is due for reapproval in accordance with Subpart D of this part.

33 CFR Part 105—MARITIME SECURITY: FACILITIES

26. The authority citation for part 105 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. 70103; 50 U.S.C. 191; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

27. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], amend § 105.115 by adding paragraph (c) to read as follows:

§ 105.115 Compliance dates.

* * * * *

(c) Facility owners or operators must:

(1) submit a TWIC Addendum to their COTP to cover each facility they own or operate subject to this part on or before [insert date 6 months after publication of final rule]; and

(2) be operating in accordance with the TWIC provisions found within this part, as outlined in their TWIC Addendum, between [insert date 1 year after publication of the final rule] and [insert date 18 months after publication of the final rule], depending on whether enrollment has been completed in the port where the facility is operating, in accordance with 49 CFR 1572.19.

28. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], amend § 105.120 by:

a. Designating the undesignated text as paragraph (a);

b. Redesignating paragraphs (a), (b), and (c) as (a)(1), (a)(2), and (a)(3), respectively; and

c. Adding paragraph (b) to read as follows:

§ 105.120 Compliance documentation.

* * * * *

(b) Each facility owner or operator subject to this part must ensure, before [insert date one year after publication of final rule] that a copies of the following documentation are available at the facility and are made available to the Coast Guard upon request:

(1) The approved TWIC addendum and any approved revisions or amendments thereto, and a letter of approval from the cognizant COTP dated within the last 5 years;

(2) The TWIC Addendum submitted for approval and current written acknowledgment from the cognizant COTP, stating that the Coast Guard is currently reviewing the TWIC Addendum submitted for approval and that the facility may continue to operate; or

(3) For facilities operating under a Coast Guard-approved Alternative Security Program as provided in §105.140, a copy of the Alternative Security Program the facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in §101.120(b)(3) of this subchapter, and a letter signed by the facility owner or operator, stating which Alternative Security Program the facility is using and certifying that the facility is in full compliance with that program, as it has been amended pursuant to §101.121 of this subchapter.

Subpart B—Facility Security Requirements

29. Revise § 105.200(b) to read as follows:

§ 105.200 Owner or operator.

* * * * *

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including;

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the area in accordance with the FSP are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Ensuring that security systems and equipment are installed and maintained, including at least one TWIC reader that meets the standard incorporated by TSA in 49 CFR 1572.23, and that computer and access control systems and hardware are secure;

(7) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(8) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(9) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of

friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can be found at http:// www.marad.dot.gov/Programs/treaties.html;

(10) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(11) Ensure security for unattended vessels moored at the facility;

(12) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter;

(13) Ensure consistency between security requirements and safety requirements;

(14) Inform facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(15) Ensure that protocols are in place for responding to TWIC holders presenting for entry who cannot electronically verify a match between themselves and the information stored on the credential's ICC. These must include interim alternative security measures for an individual who cannot electronically verify his identity. Such provisions should take into account measures appropriate for occasional failures to verify and for persistent problems with verification such that a person may require a new credential;

(16) Ensure that protocols are in place for responding to TWIC holders presenting for entry whose cards have been revoked by TSA, or other appropriate authority, or

otherwise reported as invalid, and provisions for individuals requiring access who report a lost or stolen TWIC;

(17) Ensure there are alternate provisions in case of equipment or power failures that affect TWIC readers and other validation equipment; and

(18) Ensure that appropriate personnel know who is on the facility at all times.

30. Revise § 105.205 by adding paragraphs (a)(4), (b)(2)(xv) and (c)(19) to read as follows:

§ 105.205 Facility Security Officer (FSO).

(a) * * *

(4) The FSO must maintain a valid TWIC.

(b) * * *

(2) * * *

(xv) Knowledge of TWIC.

(c) * * *

(19) Ensure the TWIC program is being properly implemented.

31. Revise § 105.210 by amending the introductory paragraph and adding paragraph (n):

§ 105.210 Facility personnel with security duties.

Facility personnel responsible for security duties must maintain a valid TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(n) Familiar with all relevant aspects of the TWIC program and how to carry them out.

32. Revise § 105.215 by adding paragraph (f):

§ 105.215 Security training for all other facility personnel.

* * * * *

(f) Familiar with all relevant aspects of the TWIC program and how to carry them out.

33. Revise § 105.225 by adding paragraph (b)(9) to read as follows:

§ 105.225 Facility recordkeeping requirements.

* * * * *

(b) * * *

(9) Records of those individuals who are granted access to the secure areas of the facility, including records of when these individuals exit the facility and, in the case of individuals who are escorted, the identification of the individual who escorted or the method by which the individual was escorted;

* * * * *

34. Revise § 105.255 to read as follows:

§ 105.255 Security measures for access control.

(a) General. The facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility;

(3) Control access to the facility; and

(4) Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area in accordance with the facility security plan.

(b) The facility owner or operator must ensure that the following are specified:

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level, including those points where a TWIC reader is or will be deployed. Each location allowing means of access to the facility must be addressed;

(2) The types of restrictions or prohibitions to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC, in accordance with 101.515, and procedures for escorting them;

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level; and

(5) The locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.

(c) The facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) Prior to granting any individual unescorted access to secure areas of the facility, ensure that the individual being granted access privileges has a TWIC and verify the individual's identity. The identity verification procedure must electronically verify a match between the individual and the biometric information stored on the TWIC's ICC. The validity of the TWIC itself shall also be verified at this time;

(2) Ensure that any individual granted unescorted access to secure areas of the facility is able to produce his or her TWIC upon request;

(3) Uses disciplinary measures to prevent fraud and abuse;

(4) Allows for temporary access if alternative security measures are implemented due to a failure of the TWIC system, and the individual can meet or pass those alternative security measures;

(5) Is coordinated, when practicable, with identification and TWIC systems of vessels or other transportation conveyances that use the facility; and

(6) Periodically verifies the validity of TWICs as outlined in paragraphs (f)(1), (g)(1) and (h)(1) of this section.

(d) If the facility owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) MARSEC Level 1. The facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section. The validity of a TWIC presented for unescorted access shall be verified using information that is no more than seven (7) days old;

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter;

(4) Check the identification of any person not holding a TWIC and seeking entry to the facility, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check shall include confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section;

(5) Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel, to establish his or her identity in accordance with this part or to account for his or her presence. Any such incident must be reported in compliance with this part;

(6) Designate restricted areas and provide appropriate access controls for these areas;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(9) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(10) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(g) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must:

(1) Verify the validity of TWIC credentials presented by all persons, using information that is no more than one (1) day old, and ensure that all TWIC enabled gates are manned; and

(2) Ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(i) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(ii) X-ray screening of all unaccompanied baggage;

(iii) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(iv) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

(v) Denying access to visitors who do not have a verified destination;

(vi) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(vii) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(h) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC level 3, the facility owner or operator must ensure that each person holding a TWIC and seeking unescorted access to a secure area is required to enter his or her correct PIN prior to being allowed to enter that area, and must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage;

(3) Being prepared to cooperate with responders and facilities;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

35. Amend § 105.280 by adding paragraph (f) to read as follows:

§ 105.280 Security incident procedures.

* * * * *

(f) Provide a list of all persons granted access to the facility, as required to be maintained in § 105.225.

36. Amend § 105.285 by revising paragraph (a)(4) to read as follows:

§ 105.285 Additional requirements-passenger and ferry facilities.

(a) * * *

(4) Deny passenger access to secure and restricted areas unless escorted by authorized facility security personnel; and

* * * * *

37. Revise § 105.290 to read as follows:

§ 105.290 Additional requirements-cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

(a) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(b) Check the identification of all persons seeking to enter the facility. Persons holding a TWIC shall be checked as set forth in this part. For persons not holding a TWIC, this check includes confirming the reason for boarding by examining passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(c) Designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects awaiting embarkation from unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area; and

(e) Deny individuals not holding a TWIC access to secure and restricted areas unless escorted.

38. Amend § 105.295 by revising paragraph (a)(1) to read as follows:

§ 105.295 Additional requirements-Certain Dangerous Cargo (CDC) facilities.

(a) * * *

(1) Escort all non-TWIC holders at all times while on the facility.

* * * * *

39. Amend § 105.296 by adding paragraph (a)(4) to read as follows:

§ 105.296 Additional requirements-barge fleeting facilities.

(a) * * *

(4) Control access to the barges once tied to the fleeting area by implementing TWIC as described in section 105.255 of this part.

* * * * *

Subpart D—Facility Security Plan (FSP)

40. Revise § 105.405(a)(10) to read as follows:

§ 105.405 Format of the Facility Security Plan (FSP).

(a) * * *

(10) Security measures for access control, including designated public access areas and TWIC implementation;

* * * * *

41. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], add Subpart E—TWIC Addendum to read as follows:

Subpart E—TWIC Addendum

105.500 General.

105.505 Submission and approval.

105.510 Integration of TWIC Addendum into full FSP.

§ 105.500 General.

A facility owner or operator must ensure the completion of a TWIC Addendum. The TWIC Addendum must outline the security measures to be used on the facility in order to implement a TWIC program as discussed in section 105.255 of this part, including the alternate procedures to be used.

§ 105.505 Submission and approval.

(a) In accordance with § 105.115, on or before [insert date six months after publication of the final rule], each facility owner or operator must either:

(1) Submit one copy of their TWIC Addendum, in English, for review and approval to the cognizant COTP and a letter certifying that their TWIC Addendum meets applicable requirements of this part; or

(2) If operating under a Coast Guard-approved Alternative Security Program (ASP), a letter signed by the facility owner or operator stating which approved ASP the owner or operator is using, and affirming that any new provisions of that ASP regarding TWIC have been implemented.

(b) Owners or operators of facilities not in service on or before [insert date of publication of the final rule] must comply with section 105.510 and submit a complete FSP that includes details regarding the implementation of a TWIC program.

(c) The cognizant COTP will examine each submission for compliance with this subpart and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) A TWIC Addendum may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.

(e) Each facility owner or operator that submits one TWIC Addendum to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility.

(f) A TWIC Addendum will be given the same expiration date as the facility's full FSP.

§ 105.510 Integration of TWIC Addendum into full FSP.

Upon gaining approval for the TWIC Addendum, the facility owner or operator must incorporate the approved TWIC Addendum into the FSP when the facility's FSP is due for reapproval in accordance with Subpart D of this part.

33 CFR Part 106—MARITIME SECURITY: OUTER CONTINENTAL SHELF (OCS) FACILITIES

42. The authority citation for part 106 continues to read as follows:

Authority: 33 U.S.C. 1226, 1231; 46 U.S.C. Chapter 701; 50 U.S.C. 191; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No, 0170.1.

43. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years] amend § 106.110 by adding paragraph (d) to read as follows:

§ 106.110 Compliance dates.

* * * * *

(d) OCS facility owners and operators must:

(1) submit a TWIC Addendum to the cognizant District Commander to cover each facility they own or operate subject to this part on or before [insert date 6 months after publication of final rule]; and

(2) be operating in accordance with the TWIC provisions found within this part, as outlined in their TWIC Addendum, between [insert date 1 year after publication of the final rule] and [insert date 18 months after publication of the final rule], depending on whether enrollment has been completed in the port where the facility is operating, in accordance with 49 CFR 1572.19.

44. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], amend § 106.115 by:

a. Designating the undesignated text as paragraph (a);

b. Redesignating paragraphs (a), (b), and (c) as (a)(1), (a)(2), and (a)(3), respectively; and

c. Adding paragraph (b) to read as follows:

§ 106.115 Compliance documentation.

* * * * *

(b) Each OCS facility owner or operator subject to this part must ensure, before [insert date one year after publication of final rule] that a copies of the following documentation are available at the OCS facility and are made available to the Coast Guard upon request:

(1) The approved TWIC addendum and any approved revisions or amendments thereto, and a letter of approval from the cognizant District Commander dated within the last 5 years;

(2) The TWIC Addendum submitted for approval and current written acknowledgment from the cognizant District Commander, stating that the Coast Guard is currently reviewing the TWIC Addendum submitted for approval and that the OCS facility may continue to operate; or

(3) For OCS facilities operating under a Coast Guard-approved Alternative Security Program as provided in §106.135, a copy of the Alternative Security Program the OCS facility is using, including a facility specific security assessment report generated under the Alternative Security Program, as specified in §101.120(b)(3) of this subchapter, and a letter signed by the OCS facility owner or operator, stating which Alternative Security Program the OCS facility is using and certifying that the OCS facility is in full compliance with that program, as it has been amended pursuant to §101.121 of this subchapter.

45. Revise § 106.200(b) to read as follows:

§ 106.200 Owner or operator.

* * * * *

(b) For each OCS facility, the OCS facility owner or operator must:

(1) Define the security organizational structure for each OCS Facility and provide each person exercising security duties or responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate in writing, by name or title, a Company Security Officer (CSO) and a Facility Security Officer (FSO) for each OCS Facility and identify how those officers can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of a Facility Security Plan (FSP);

(5) Ensure that the OCS facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including:

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the area in accordance with the OCS FSP are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Ensuring that security systems and equipment are installed and maintained, including at least one TWIC reader that meets the standard incorporated by TSA in 49 CFR 1572.23, and that computer and access control systems and hardware are secure;

(7) Ensure that adequate coordination of security issues takes place between OCS facilities and vessels, including the execution of a Declaration of Security (DoS) as required by this part;

(8) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required by the FSP for the new MARSEC Level;

(9) Ensure all breaches of security and security incidents are reported in accordance with part 101 of this subchapter;

(10) Ensure consistency between security requirements and safety requirements;

(11) Inform OCS facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(12) Ensure that protocols are in place for responding to TWIC holders presenting for entry who cannot electronically verify a match between themselves and the biometric information stored on the credential's ICC. These must include interim alternative security measures for an individual who cannot electronically identify his identity. Such provisions should take into account measures appropriate for occasional failures to verify and for persistent problems with verification such that a person may require a new credential;

(13) Ensure that protocols are in place for responding to TWIC holders presenting for entry whose cards have been revoked by TSA, or other appropriate authority, or otherwise reported as invalid, and provisions for individuals requiring access who report a lost or stolen TWIC;

(14) Ensure there are alternate provisions in case of equipment or power failures that affect TWIC readers and other validation equipment; and

(15) Ensure that appropriate personnel know who is on the OCS facility at all times.

46. Revise § 106.205 by adding paragraphs (a)(4), (c)(13) and (d)(13) to read as follows:

§ 106.205 Company Security Officer (CSO).

(a) * * *

(4) The CSO must maintain a valid TWIC.

* * * * *

(c) * * *

(13) Knowledge of TWIC.

(d) * * *

(13) Ensure the TWIC program is being properly implemented.

47. Revise § 106.210 by adding paragraphs (a)(4) and (c)(15) to read as follows:

§ 106.210 OCS Facility Security Officer (FSO).

(a) * * *

(4) The FSO must maintain a valid TWIC.

* * * * *

(c) * * *

(15) Ensure the TWIC programs is properly implemented.

48. Revise § 106.215 by amending the introductory paragraph and redesignating paragraphs (k) and (l) as (l) and (m), respectively, and adding new paragraph (k) to read as follows:

§ 106.215 Company of OCS facility personnel with security duties.

Company and OCS facility personnel responsible for security duties must maintain a valid TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

* * * * *

(k) Familiarity with all relevant aspects of the TWIC program and how to carry them out;

* * * * *

49. Revise § 106.220 by adding paragraph (f) to read as follows:

§ 106.220 Security training for all other OCS personnel.

* * * * *

(f) Familiarity with all relevant aspects of the TWIC program and how to carry them out.

50. Revise § 106.230 by adding paragraph (b)(9) to read as follows:

§ 106.230 OCS facility recordkeeping requirements.

* * * * *

(b)* * *

(9) Records of those individuals who are granted access to the secure area of the OCS facility, including records of when these individuals exit the OCS facility and, in the case of individuals who are escorted, the identification of the individual who escorted or the method by which the individual was escorted.

51. Revise § 106.260 to read as follows:

§ 106.260 Security measures for access control.

(a) General. The OCS facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, or the OCS facility;

(2) Secure dangerous substances and devices that are authorized by the OCS facility owner or operator to be on board;

(3) Control access to the OCS facility; and

(4) Prevent an unescorted individual from entering the OCS facility unless the individual holds a duly issued TWIC and is authorized to be on the OCS facility in accordance with the OCS facility security plan.

(b) The OCS facility owner or operator must ensure that the following are specified:

(1) All locations providing means of access to the OCS facility where access restrictions or prohibitions are applied for each security level to prevent unauthorized access, including those points where a TWIC reader is or will be deployed;

(2) The identification of the types of restriction or prohibition to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC and the means by which they will be allowed access to the OCS facility; and

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level.

(c) The OCS facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) Prior to granting any individual unescorted access to the OCS facility, ensure that the individual has a TWIC and verify the individual's identity. The identity verification procedure must electronically verify a match between the individual and the biometric information stored on the TWIC's ICC. The validity of the TWIC itself must also be verified at this time;

(2) Ensure that any individual granted unescorted access to the OCS facility is able to produce his or her TWIC upon request;

(3) Uses disciplinary measures to prevent fraud and abuse;

(4) Allows for temporary access if alternative security measures are implemented due to a failure of the TWIC system, and the individual can meet or pass those alternative security measures; and

(5) Periodically verifies the validity of TWICs, using the latest information available from TSA, as outlined in paragraphs (f)(1), (g)(1) and (h)(1) of this section.

(d) If the OCS facility owner or operator uses a separate identification system, ensure that it is coordinated with identification and TWIC systems in place on vessels conducting operations with the OCS facility.

(e) The OCS facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) MARSEC Level 1. The OCS facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section. The validity of a TWIC presented for unescorted access shall be verified using information that is no more

than seven (7) days old. The validity of a TWIC held by a person already granted access to the OCS facility shall be verified weekly, using the most current information available from TSA;

(2) Screen persons and personal effects going aboard the OCS facility for dangerous substances and devices at the rate specified in the approved FSP;

(3) Conspicuously post signs that describe security measures currently in effect and clearly stating that:

(i) Boarding an OCS facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to be on board;

(4) Check the identification of any person seeking to board the OCS facility, including OCS facility employees, passengers and crews of vessels interfacing with the OCS facility, vendors, and visitors and ensure that non-TWIC holders are denied unescorted access to the OCS facility;

(5) Deny or revoke a person's authorization to be on board if the person is unable or unwilling, upon the request of OCS facility personnel, to establish his or her identity in accordance with this part or to account for his or her presence on board. Any such incident must be reported in compliance with this part;

(6) Deter unauthorized access to the OCS facility;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Lock or otherwise prevent access to unattended spaces that adjoin areas to which OCS facility personnel and visitors have access;

(9) Ensure OCS facility personnel are not required to engage in or be subjected to screening, of the person or of personal effects, by other OCS facility personnel, unless security clearly requires it;

(10) Provide a designated secure area on board, or in liaison with a vessel interfacing with the OCS facility, for conducting inspections and screening of people and their personal effects; and

(11) Respond to the presence of unauthorized persons on board.

(g) MARSEC Level 2. In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the OCS facility owner or operator must:

(1) Verify the validity of a TWIC presented for unescorted access shall be verified using information that is no more than one (1) day old, and verify the validity of a TWIC held by a person already granted access to the OCS facility daily, using the most current information available from TSA;

(2) Ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(i) Increasing the frequency and detail of screening of people and personal effects embarking onto the OCS facility as specified for MARSEC Level 2 in the approved FSP;

(ii) Assigning additional personnel to patrol deck areas during periods of reduced OCS facility operations to deter unauthorized access;

(iii) Limiting the number of access points to the OCS facility by closing and securing some access points; or

(iv) Deterring waterside access to the OCS facility, which may include, providing boat patrols.

(h) MARSEC Level 3. In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC level 3, the facility owner or operator must ensure that each person holding a TWIC and seeking unescorted access to a secure area is required to enter his or her correct PIN prior to being allowed to enter that area, and must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. The additional security measures may include:

(1) Screening all persons and personal effects for dangerous substances and devices;

(2) Being prepared to cooperate with responders;

(3) Limiting access to the OCS facility to a single, controlled access point;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending embarkation and/or disembarkation of personnel;

(6) Suspending the loading of stores or industrial supplies;

(7) Evacuating the OCS facility; or

(8) Preparing for a full or partial search of the OCS facility.

52. Amend § 106.280 by adding paragraph (g) to read as follows:

§ 106.280 Security incident procedures.

* * * * *

(g) Provide a list of all persons granted access to the OCS facility, as required to be maintained in § 106.230.

Subpart D—Outer Continental Shelf (OCS) Facility Security Plan (FSP)

53. Revise § 106.405(a)(10) to read as follows:

§ 106.405 Format of the Facility Security Plan (FSP).

(a) * * *

(10) Security measures for access control, including TWIC implementation;

* * * * *

54. From [insert effective date of the final rule] to [insert effective date of final rule + 5 years], add Subpart E—TWIC Addendum to read as follows:

Subpart E—TWIC Addendum

106.500 General.

106.505 Submission and approval.

106.510 Integration of TWIC Addendum into full FSP.

§ 106.500 General.

An OCS facility owner or operator must ensure the completion of a TWIC Addendum. The TWIC Addendum must outline the security measures to be used on the OCS facility in order to implement a TWIC program as discussed in section 106.260 of this part, including the alternate procedures to be used.

§ 106.505 Submission and approval.

(a) In accordance with § 106.115, on or before [insert date six months after date of publication of final rule], each OCS facility owner or operator must either:

(1) Submit one copy of their TWIC Addendum, in English, for review and approval to the cognizant District Commander and a letter certifying that their TWIC Addendum meets applicable requirements of this part; or

(2) If operating under a Coast Guard-approved Alternative Security Program (ASP), a letter signed by the OCS facility owner or operator stating which approved ASP the owner or operator is using, and affirming that any new provisions of that ASP regarding TWIC have been implemented.

(b) Owners or operators of OCS facilities not in service on or before [insert date of publication of final rule] must comply with section 106.510 and submit a complete FSP that includes details regarding the implementation of a TWIC program.

(c) The cognizant District Commander will examine each submission for compliance with this subpart and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) A TWIC Addendum may be submitted and approved to cover more than one facility where they share similarities in physical characteristics, location, and operations.

(e) Each OCS facility owner or operator that submits one TWIC Addendum to cover two or more OCS facilities of similar design, location, and operation must address OCS facility-specific information that includes the physical and operational characteristics of each OCS facility.

(f) A TWIC Addendum will be given the same expiration date as the OCS facility's full FSP.

§ 106.510 Integration of TWIC Addendum into full FSP.

Upon gaining approval for the TWIC Addendum, the OCS facility owner or operator must incorporate the approved TWIC Addendum into the FSP when the OCS facility's FSP is due for reapproval in accordance with Subpart D of this part.

PART 125—IDENTIFICATION CREDENTIALS FOR PERSONS REQUIRING ACCESS TO WATERFRONT FACILITIES OR VESSELS

55. The authority citation for part 125 is revised to read as follows:

Authority: R.S. 4517, 4518, secs. 19, 2, 23 Stat. 58, 118, sec. 7, 49 Stat. 1936, sec. 1, 40 Stat. 220; 46 U.S.C. 570–572, 2, 689, and 70105; 50 U.S.C. 191, EO 10173, EO 10277, EO 10352, 3 CFR, 1949–1953 Comp. pp. 356, 778, 873.

56. In §125.09, revise paragraph (f) and add paragraph (g) to read as follows:

§ 125.09 Identification credentials.

* * * * *

(a) * * *

(f) Transportation Worker Identification Credential.

(g) Such other identification as may be approved by the Commandant from time to time.

* * * * *

46 CFR PART 10—LICENSING OF MARITIME PERSONEL

57. The authority citation for part 10 continues to read as follows:

Authority: 14 U.S.C. 633; 31 U.S.C. 9701; 46 U.S.C. 2101, 2103, and 2110; 46 U.S.C. chapter 71; 46 U.S.C. 7502, 7505, 7701, and 8906; Executive Order 10173;

Department of Homeland Security Delegation No. 0170.1. Section 11.107 is also issued under the authority of 44 U.S.C. 3507.

58. Add new § 10.113 to read as follows:

§ 10.113 Transportation Worker Identification Credential

In accordance with the implementation schedule contained in 49 CFR 1572.19, all mariners holding an active License, Certificate of Registry or STCW endorsement issued under this Part must hold a valid Transportation Worker Identification Credential (TWIC) issued by the Transportation Security Administration under title 49 CFR part 1572.

46 CFR PART 12—CERTIFICATION OF SEAMEN

59. The authority citation for part 12 is revised to read as follows:

Authority: 31 U.S.C. 9701; 46 U.S.C. 2101, 2103, 2110, 7301, 7302, 7503, 7505, 7701, and 70105; Department of Homeland Security Delegation No. 0170.1.

60. Add new § 12.01-11 to read as follows:

§ 12.01-11 Transportation Worker Identification Credential

In accordance with the implementation schedule contained in 49 CFR 1572.19, all mariners holding a Merchant Mariner's Document or STCW endorsement issued under this Part must hold a valid Transportation Worker Identification Credential (TWIC) issued by the Transportation Security Administration under title 49 CFR part 1572.

PART 15—MANNING REQUIREMENTS

61. The authority citation for part 15 is revised to read as follows:

Authority: 46 U.S.C. 2101, 2103, 3306, 3703, 8101, 8102, 8104, 8105, 8301, 8304, 8502, 8503, 8701, 8702, 8901, 8902, 8903, 8904, 8905(b), 8906, 9102, and 70105; and Department of Homeland Security Delegation No. 0170.1.

62. Add new § 15.415 to read as follows:

§ 15.415 Transportation Worker Identification Credential

In accordance with the implementation schedule contained in 49 CFR 1572.19, a person may not employ or engage an individual, and an individual may not serve in a position in which an individual is required by law or regulation to hold an active License, Merchant Mariner Document, Certificate of Registry or STCW endorsement, unless the individual holds a valid Transportation Security Identification Credential (TWIC). All mariners holding an active License, Merchant Mariner Document, Certificate of Registry or STCW endorsement issued by the Coast Guard must hold a valid TWIC issued by the Transportation Security Administration under title 49 CFR part 1572.

TRANSPORTATION SECURITY ADMINISTRATION

49 CFR CHAPTER XII

63. Add a new part 1515 to subchapter A to read as follows:

SUBCHAPTER A—ADMINISTRATIVE AND PROCEDURAL RULES

PART 1515—APPEAL AND WAIVER PROCEDURES FOR SECURITY THREAT ASSESSMENTS FOR INDIVIDUALS

Sec.

1515.7 Waiver procedures.

Authority**:** 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

PART 1515—APPEAL AND WAIVER PROCEDURES FOR SECURITY THREAT ASSESSMENTS FOR INDIVIDUALS

§ 1515.1 Scope.

This part applies to applicants who undergo one of the following security threat assessments and wish to appeal an Initial Determination of Threat Assessment or an Initial Determination of Threat Assessment and Immediate Revocation or apply for a waiver:

(a) For a hazardous materials endorsement (HME) as described in 49 CFR part 1572.

(b) For a Transportation Worker Identification Credential (TWIC) as described in 49 CFR part 1572.

§ 1515.3 Terms used in this part.

The terms used in 49 CFR parts 1500, 1540, 1570, and 1572 also apply in this part. In addition, the following terms are used in this part:

Applicant means a person who has applied for one of the security threat assessments identified in § 1515.1

Date of service means—

(1) In the case of personal service, the date of personal delivery to the residential address listed on the application;

(2) In the case of mailing with a certificate of service, the date shown on the certificate of service;

(3) In the case of mailing and there is no certificate of service, 10 days from the date mailed to the address designated on the application as the mailing address;

(4) In the case of mailing with no certificate of service or postmark, the date mailed to the address designated on the application as the mailing address shown by other evidence; or

(5) The date on which an electronic transmission occurs.

Day means calendar day.

Security threat assessment means the threat assessment for which the applicant has applied, as described in § 1515.1.

§ 1515.5 Appeal procedures.

(a) Scope. This section applies to appeals from an Initial Determination of Threat--

(1) For a hazardous materials endorsement (HME) as described in 49 CFR 1572.15.

(2) For a Transportation Worker Identification Credential (TWIC) as described in 49 CFR 1572.15.

(b) Grounds for appeal. An applicant may appeal an Initial Determination of Threat Assessment if the applicant is asserting that he or she meets the standards for the security threat assessment for which he or she is applying.

(c) Appeal. (1) Initiating an appeal. An applicant initiates an appeal by submitting a written reply to TSA or written request for materials from TSA. If the

applicant does not initiate an appeal within 60 days of receipt, the Initial Determination of Threat Assessment becomes final. TSA then serves a Final Determination of Threat Assessment on the applicant.

(i) In the case of an HME, TSA also serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a mariner applying for TWIC, TSA also serves a Final Determination of Threat Assessment on the Coast Guard.

(2) Request for materials. Within 60 days of the date of service of the Initial Determination of Threat Assessment, the applicant may serve upon TSA a written request for copies of the materials upon which the Initial Determination was based.

(3) TSA response. (i) Within 60 days of receiving the applicant's request for materials, TSA serves copies of the releasable materials upon the applicant on which the Initial Determination was based. TSA will not include any classified information or other protected information described in paragraph (f) of this section.

(ii) Within 60 days of receiving the applicant's request for materials or written reply, TSA may request additional information or documents from the applicant that TSA believes are necessary to make a Final Determination.

(4) Correction of records. If the Initial Determination of Threat Assessment was based on a record that the applicant believes is erroneous, the applicant may correct the record, as follows:

(i) The applicant contacts the jurisdiction or entity responsible for the information and attempts to correct or complete information contained in his or her record.

(ii) The applicant provides TSA with the revised record, or a certified true copy of the information from the appropriate entity, before TSA determines that the applicant meets the standards for the security threat assessment.

(5) Reply. (i) The applicant may serve upon TSA a written reply to the Initial Determination of Threat Assessment within 60 days of service of the Initial Determination, or 60 days after the date of service of TSA's response to the applicant's request for materials under paragraph (b)(1) of this section, if the applicant served such request. The reply must include the rationale and information on which the applicant disputes TSA's Initial Determination.

(ii) In an applicant's reply, TSA will consider only material that is relevant to whether the applicant meets the standards described in § 1572.5(a).

(6) Final determination. Within 60 days after TSA receives the applicant's reply, TSA serves a Final Determination of Threat Assessment or a Withdrawal of the Initial Determination as provided in paragraphs (c) or (d) of this section.

(d) Final Determination of Threat Assessment. (1) If the Director concludes that the applicant does not meet the standards described in § 1572.5(a)(1), (a)(2), or (a)(4) following an appeal, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition--

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a mariner applying for TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the Federal Maritime Security Coordinator (FMSC).

(2) If the Assistant Secretary concludes that the applicant does not meet the security threat assessment standards described in § 1572.5(a)(3) following an appeal, TSA serves a Final Determination of Threat Assessment upon the applicant. In addition—

(i) In the case of an HME, TSA serves a Final Determination of Threat Assessment on the licensing State.

(ii) In the case of a mariner applying for TWIC, TSA serves a Final Determination of Threat Assessment on the Coast Guard.

(iii) In the case of a TWIC, TSA serves a Final Determination of Threat Assessment on the FMSC.

(3) The Final Determination includes a statement that the Director or Assistant Secretary has reviewed the Initial Determination, the applicant's reply and any accompanying information, and any other materials or information available to him or her, and has determined that the applicant poses a security threat warranting denial of the security threat assessment for which the applicant has applied.

(e) Withdrawal of Initial Determination. If the Director or Assistant Secretary concludes that the applicant does not pose a security threat, TSA serves a Withdrawal of the Initial Determination upon the applicant.

(f) Nondisclosure of certain information. In connection with the procedures under this section, TSA does not disclose classified information to the applicant, as defined in

Executive Order 12968 section 1.1(d), and reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

(g) Extension of time. TSA may grant an applicant an extension of time of the limits described in this section for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended. TSA may grant itself an extension of time for good cause.

(h) Judicial review. For purposes of judicial review, the Final Determination of Threat Assessment constitutes a final TSA order in accordance with 49 U.S.C. 46110.

(i) Appeal of immediate revocation. If TSA directs an immediate revocation, the applicant may appeal this determination by following the appeal procedures described in paragraph (b) of this section. This applies to—

(i) If TSA directs a State to revoke an HME pursuant to § 1572.13(a).

(ii) If TSA invalidates a TWIC by issuing an Initial Determination of Threat Assessment and Immediate Revocation pursuant to § 1572.21(d)(3).

§ 1515.7 Waiver procedures.

(a) Scope. This section applies if an applicant does not meet certain standards for a security threat assessment but wishes to obtain a waiver of those standards, for--

(1) For a hazardous materials endorsement (HME) as described in 49 CFR part 1572.

(2) For a Transportation Worker Identification Credential (TWIC) as described in 49 CFR part 1572.

(b) Grounds for waiver. TSA may issue a waiver of certain standards and grant an HME or TWIC, if TSA determines that an applicant no longer poses a security threat based on a review of information described in paragraph (c) of this section. An applicant disqualified for the reasons described in paragraphs (b)(1) through (b)(3) of this section may apply for a waiver of the standards.

(1) A disqualifying criminal offense described in §§ 1572.103(a)(5) through (a)(9), and § 1572.103(a)(10), if the underlying criminal offense is in §§ 1572.103 (a)(5) through (a)(9); or

(2) A disqualifying criminal offense described in § 1572.103(b); or

(3) Mental incapacity as described in § 1572.109.

(c) Initiating waiver. (1) An applicant initiates a waiver request by--

(i) Providing the information required in § 1572.9 for an HME or § 1572.17 for a TWIC;

(ii) Paying the fees required in § 1572.405 (a)(1)-(a)(3) for an HME or in § 1572.503(a)(i)-(a)(iii) for a TWIC; and

(iii) Sending a written request to TSA for a waiver at any time, but not later than 60 days after the date of service of the Final Determination of Threat Assessment.

(2) In determining whether to grant a waiver, TSA will consider the following factors:

(i) The circumstances of the disqualifying act or offense.

(ii) Restitution made by the applicant.

(iii) Any Federal or State mitigation remedies.

(iv) Court records or official medical release documents indicating that the individual no longer lacks mental capacity.

(v) Other factors that indicate the applicant does not pose a security threat warranting denial of the HME or TWIC.

(d) Grant or denial of waivers. (1) The Director will send a written decision granting or denying the waiver to the applicant within 60 days of service the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(2) In the case of an HME, if the Director grants the waiver, the Director will send a Determination of No Security Threat to the licensing State within 60 days of service the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(3) In the case of a mariner applying for TWIC, if the Director grants the waiver, the Director will send a Determination of No Security Threat to the Coast Guard within 60 days of service the applicant's request for a waiver, or longer period as TSA may determine for good cause.

(e) Extension of time. TSA may grant an applicant an extension of time of the limits described in paragraph (b) and (c) of this section for good cause shown. An applicant's request for an extension of time must be in writing and be received by TSA within a reasonable time before the due date to be extended. TSA may grant itself an extension of time for good cause.

SUBCHAPTER D—MARITIME AND LAND TRANSPORTATION SECURITY

64. Revise part 1570 to read as follows:

PART 1570—GENERAL RULES

Sec.

Authority: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

PART 1570—GENERAL RULES

§ 1570.1 Scope.

This part applies to any person involved in land or maritime transportation as specified in this part.

§ 1570.3 Terms used in this subchapter.

For purposes of the subchapter:

Adjudicate means to make an administrative determination of whether an applicant meets the standards in this subchapter, based on the merits of the issues raised.

Alien means any person not a citizen or national of the United States.

Alien registration number means the number issued by the U.S. Department of Homeland Security to an individual when he or she becomes a lawful permanent resident of the United States or attains other lawful, non-citizen status.

Applicant means a person who has applied for one of the security threat assessments identified in this subchapter.

Assistant Secretary means Assistant Secretary for Homeland Security, Transportation Security Administration (Assistant Secretary), the highest ranking TSA official, or his or her designee, and who is responsible for making the final determination on the appeal of an intelligence-related check under this part.

Commercial drivers license (CDL) is used as defined in 49 CFR 383.5.

Convicted means any plea of guilty or nolo contendere, or any finding of guilt, except when the finding of guilt is subsequently overturned on appeal, pardoned, or expunged. For purposes of this subchapter, a conviction is expunged when the conviction is removed from the individual's criminal history record and there are no legal disabilities or restrictions associated with the expunged conviction, other than the fact that the conviction may be used for sentencing purposes for subsequent convictions. In addition, where an individual is allowed to withdraw an original plea of guilty or nolo contendere and enter a plea of not guilty and the case is subsequently dismissed, the individual is no longer considered to have a conviction for purposes of this subchapter.

Determination of No Security Threat means an administrative determination by TSA that an individual does not pose a security threat warranting denial of an HME or a TWIC.

Director means the officer designated by the Assistant Secretary to administer the appeal and waiver programs described in this part, except where the Assistant Secretary is specifically designated in this part to administer the appeal or waiver program. The Director may appoint a designee to assume his or her duties.

Federal Maritime Security Coordinator (FMSC) has the same meaning as defined in 46 U.S.C. 70103(a)(2)(G); is the Captain of the Port (COTP) exercising authority for the COTP zones described in 33 CFR part 3, and is the Port Facility Security Officer as described in the International Ship and Port Facility Security (ISPS) Code, part A.

Final Determination of Threat Assessment means a final administrative determination by TSA, including the resolution of related appeals, that an individual poses a security threat warranting denial of an HME or a TWIC.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, an indication of which must be on the individual's commercial driver's license, as provided in the Federal Motor Carrier Safety Administration (FMCSA) regulations in 49 CFR part 383.

Imprisoned or imprisonment means confined to a prison, jail, or institution for the criminally insane, on a full-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity. Time spent confined or restricted to a half-way house, treatment facility, or similar institution, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity, does not constitute imprisonment for purposes of this rule.

Incarceration means confined or otherwise restricted to a jail-type institution, half-way house, treatment facility, or another institution, on a full or part-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity.

Initial Determination of Threat Assessment means an initial administrative determination by TSA that an individual poses pose a security threat warranting denial of an HME or a TWIC.

Initial Determination of Threat Assessment and Immediate Revocation means an initial administrative determination that an individual poses a security threat that warrants immediate revocation of an HME or invalidation of a TWIC. In the case of an HME, the

State must immediately revoke the HME if TSA issues an Initial Determination of Threat Assessment and Immediate Revocation. In the case of a TWIC, TSA invalidates the TWIC when TSA issues an Initial Determination of Threat Assessment and Immediate Revocation.

Invalidate means the action TSA takes to make a credential inoperative when it is reported as lost, stolen, damaged, no longer needed, or when TSA determines an applicant does not meet the security threat assessment standards of part 1572.

Lawful permanent resident means an individual, lawfully admitted to the United States for permanent residence, as defined in 8 U.S.C. 1101.

Maritime facility has the same meaning as "facility" together with "OCS facility" (Outer Continental Shelf facility), as defined in 33 CFR 101.105.

Mental health facility means a mental institution, mental hospital, sanitarium, psychiatric facility, and any other facility that provides diagnoses by licensed professionals of mental retardation or mental illness, including a psychiatric ward in a general hospital.

Owner/operator with respect to a maritime facility or a vessel has the same meaning as defined in 33 CFR 101.105.

Revocation means the termination, deactivation, rescission, invalidation, cancellation, or withdrawal of the privileges and duties conferred by an HME or TWIC, when TSA determines an applicant does not meet the security threat assessment standards of part 1572.

Secure area means the area on board a vessel or at a facility or outer continental shelf facility, over which the owner/operator has implemented security measures for

access control, as defined by a Coast Guard approved security plan. It does not include passenger access areas or public access areas, as those terms are defined in 33 CFR 104.106 and 105.106 respectively.

Security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

Sensitive security information (SSI) means information that is described in, and must be managed in accordance with, 49 CFR part 1520.

State means a State of the United States and the District of Columbia.

Transportation Worker Identification Credential (TWIC) means a Federal biometric credential, issued to an individual, when TSA determines that the individual does not pose security threat.

Withdrawal of Initial Determination of Threat Assessment is the document that TSA issues after issuing an Initial Determination of Security Threat, when TSA determines that an individual does not pose a security threat, warranting denial of an HME or TWIC.

§ 1570.5 Fraud and intentional falsification of records.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with the subchapter, or exercise any privileges under this subchapter.

(b) Any reproduction or alteration, for fraudulent purpose, of any record, report, security program, access medium, or identification medium issued under this subchapter or pursuant to standards in this subchapter.

65. Revise part 1572 to read as follows:

PART 1572—CREDENTIALING AND SECURITY THREAT ASSESSMENTS

Subpart A--Procedures and General Standards

Sec.

Subpart B--Qualification Standards for Security Threat Assessments

Authority: 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; 18 U.S.C. 842, 845; 6 U.S.C. 469.

PART 1572—CREDENTIALING AND SECURITY THREAT ASSESSMENTS

Subpart A--Procedures and General Standards

§ 1572.1 Applicability.

This part establishes regulations for credentialing and security threat assessments for certain maritime and land transportation workers.

§ 1572.3 Scope.

This part applies to—

(a) State agencies responsible for issuing a hazardous materials endorsement (HME); and

(b) An applicant who—

(1) Is qualified to hold a commercial driver's license under 49 CFR parts 383 and 384, and is applying to obtain, renew, or transfer an HME; or

(2) Is applying to obtain or renew a TWIC in accordance with 33 CFR parts 104-106 or 46 CFR part 10;

§ 1572.5 Standards for security threat assessments.

(a) Standards. TSA determines that an applicant poses a security threat warranting denial of an HME or TWIC, if--

(1) The applicant has a disqualifying criminal offense described in § 1572.103;

(2) The applicant does not meet the immigration status requirements described in § 1572.105;

(3) TSA conducts the analyses described in § 1572.107 and determines that the applicant poses a security threat; or

(4) The applicant has been adjudicated as lacking mental capacity or committed to a mental health facility, as described in § 1572.109.

(b) Immediate Revocation/Invalidation. TSA may invalidate a TWIC or direct a State to revoke an HME immediately, if TSA determines during the security threat assessment that an applicant poses an immediate threat to transportation security, national security, or of terrorism.

(c) Violation of FMCSA Standards. The regulations of the Federal Motor Carrier Safety Administration (FMCSA) provide that an applicant is disqualified from operating a commercial motor vehicle for specified periods, if he or she has an offense that is listed in the FMCSA rules at 49 CFR 383.51. If records indicate that an applicant has committed an offense that would disqualify the applicant from operating a commercial motor vehicle under 49 CFR 383.51, TSA will not issue a Determination of No Security Threat until the State or the FMCSA determine that the applicant is not disqualified under that section.

(d) Comparability of Other Security Threat Assessment Standards. TSA may determine that security threat assessments conducted by other governmental agencies are comparable to the threat assessment described in this part, which TSA conducts for HME and TWIC applicants.

(1) In making a comparability determination, TSA will consider—

(i) The minimum standards used for the security threat assessment;

(ii) The frequency of the threat assessment;

(iii) The date of the most recent threat assessment; and

(iv) Whether the threat assessment includes biometric identification and a biometric credential.

(2) To apply for a comparability determination, the agency seeking the determination must contact the Assistant Program Manager, Attn: Federal Agency Comparability Check, Hazmat Threat Assessment Program, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220.

(3) TSA will notify the public when a comparability determination is made.

(4) An applicant, who has completed a security threat assessment that is determined to be comparable under this section to the threat assessment described in this part, must complete the enrollment process and provide biometric information to obtain a TWIC, if the applicant seeks unescorted access to a secure area of a vessel or facility. The applicant must pay the fee listed in § 1572.503 for information collection/credential issuance.

(5) TSA has determined that the security threat assessment for an HME under this part is comparable to the security threat assessment for TWIC.

(6) TSA has determined that the security threat assessment for a FAST card, under the Free and Secure Trade program administered by the U.S. Customs and Border Protection, is comparable to the security threat assessment described in this part.

§ 1572.7 Waiver of security threat assessment standards.

(a) An applicant may apply to TSA for a waiver of the standards described in § 1572.5, if the applicant—

(1) Has a disqualifying criminal offense described in §§ 1572.103(a)(5) through (a)(9), and § 1572.103 (a)(10), if the underlying criminal offense is in §§ 1572.103 (a)(5) through (a)(9); or

(2) Has a disqualifying criminal offense described in § 1572.103(b); or

(3) Has a history of mental incapacity described in § 1572.109.

(b) HME and TWIC applicants must follow the procedures described in 49 CFR 1515.7 when applying for a waiver.

§ 1572.9 Applicant information required for HME security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew an HME. When applying to transfer an HME from one State to another, § 1572.13(e) applies.

(a) The applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and email address.

(3) Date of birth.

(4) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(5) Gender.

(6) Height, weight, hair color, and eye color.

(7) City, state, and country of birth.

(8) Immigration status and, if the applicant is a naturalized citizen of the United States, the date of naturalization.

(9) Alien registration number, if applicable.

(10) The State of application, CDL number, and type of HME(s) held.

(11) Name, telephone number, facsimile number, and address of the applicant's current employer(s), if the applicant's work for the employer(s) requires an HME.

(b) The applicant must provide a statement, signature, and date of signature that he or she—

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in § 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in § 1572.103(b), during the five years before the date of the application;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in § 1572.103;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in § 1572.103(a), in a civilian or military jurisdiction;

(5) Has not been adjudicated as lacking mental capacity or committed to a mental health facility involuntarily;

(6) Meets the immigration status requirements described in § 1572.105;

(7) Has or has not served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations, under § 1572.11, impose a continuing obligation on the HME holder to disclose to the State if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. **Purpose:** This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a hazardous materials endorsement for a commercial driver's license. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. **Routine Uses:** Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(d) The applicant must certify and date receipt the following statement, immediately before the signature line:

> The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application can be punished by fine or imprisonment or both (See section 1001 of Title 18 United States Code), and may be grounds for denial of a hazardous materials endorsement.

(e) The applicant must certify the following statement in writing:

> I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified.

§ 1572.11 Applicant responsibilities for HME security threat assessment.

(a) Surrender of HME. If an individual is disqualified from holding an HME under § 1572.5(c), he or she must surrender the HME to the licensing State. Failure to surrender the HME to the State may result in immediate revocation under § 1572.13(a) and/or civil penalties.

(b) Continuing responsibilities. An individual who holds an HME must surrender the HME as required in paragraph (a) of this section within 24 hours, if the individual--

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in § 1572.103; or

(2) Is adjudicated as lacking mental capacity, or committed to a mental health facility, as described in § 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status, and/or is ordered removed from the United States.

(c) Submission of fingerprints and information. (1) An HME applicant must submit fingerprints and the information required in § 1572.9, in a form acceptable to TSA, when so notified by the State, or when the applicant applies to obtain or renew an HME. The procedures outlined in § 1572.13(e) apply to HME transfers.

(2) When submitting fingerprints and the information required in § 1572.9, the fee described in § 1572.503 must be remitted to TSA.

§ 1572.13 State responsibilities for issuance of hazardous materials endorsement.

Each State must revoke an individual's HME immediately, if TSA informs the State that the individual does not meet the standards for security threat assessment in § 1572.5 and issues an Initial Determination of Threat Assessment and Immediate Revocation.

(a) No State may issue or renew an HME for a CDL, unless the State receives a Determination of No Security Threat from TSA.

(b) Each State must notify each individual holding an HME issued by that State that he or she will be subject to the security threat assessment described in this part as part of an application for renewal of the HME, at least 60 days prior to the expiration date of the individual's HME. The notice must inform the individual that he or she may initiate the security threat assessment required by this section at any time after receiving the notice, but no later than 60 days before the expiration date of the individual's HME.

(c) The State that issued an HME may extend the expiration date of the HME for 90 days, if TSA has not provided a Determination of No Security Threat or a Final Determination of Threat Assessment before the expiration date. Any additional extension must be approved in advance by TSA.

(d) Within 15 days of receipt of a Determination of No Security Threat or Final Determination of Threat Assessment from TSA, the State must—

(1) Update the applicant's permanent record to reflect:

(i) The results of the security threat assessment;

(ii) The issuance or denial of an HME; and

(iii) The new expiration date of the HME.

(2) Notify the Commercial Drivers License Information System operator of the results of the security threat assessment.

(3) Revoke or deny the applicant's HME if TSA serves the State with a Final Determination of Threat Assessment.

(e) For applicants who apply to transfer an existing HME from one State to another, the second State will not require the applicant to undergo a new security threat

assessment until the security threat assessment renewal period established in the preceding issuing State, not to exceed five years, expires.

(f) Each State must retain the application and information required in § 1572.9, for at least one year, in paper or electronic form.

§ 1572.15 Procedures for HME security threat assessment.

(a) Contents of security threat assessment. The security threat assessment TSA completes includes a fingerprint-based criminal history records check, an intelligence-related background check, and a final disposition.

(b) Fingerprint-based check. In order to conduct a fingerprint-based criminal history records check, the following procedures must be completed:

(1) The State notifies the applicant that he or she will be subject to the security threat assessment at least 60 days prior to the expiration of the applicant's HME, and that the applicant must begin the security threat assessment no later than 30 days before the date of the expiration of the HME.

(2) Where the State elects to collect fingerprints and applicant information, the State—

(i) Collects fingerprints and applicant information required in § 1572.9;

(ii) Provides the applicant information to TSA electronically, unless otherwise authorized by TSA;

(iii) Transmits the fingerprints to the FBI/Criminal Justice Information Services (CJIS), in accordance with the FBI/CJIS fingerprint submission standards; and

(iv) Retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested.

(3) Where the State elects to have a TSA agent collect fingerprints and applicant information—

(i) TSA provides a copy of the signed application to the State;

(ii) The State retains the signed application, in paper or electronic form, for one year and provides it to TSA, if requested; and

(iii) TSA transmits the fingerprints to the FBI/CJIS, in accordance with the FBI/CJIS fingerprint submission standards.

(4) TSA receives the results from the FBI/CJIS and adjudicates the results of the check, in accordance with § 1572.103 and, if applicable, § 1572.107.

(c) Intelligence-related check. To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in § 1572.9.

(2) Searches domestic and international Government databases described in §§ 1572.105, 1572.107, and 1572.109.

(3) Adjudicates the results of the check in accordance with §§ 1572.103, 1572.105, 1572.107, and 1572.109.

(d) Final disposition. Following completion of the procedures described in paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the State in which the applicant is authorized to hold an HME, if TSA determines that an applicant meets the security threat assessment standards described in § 1572.5.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant, if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1515.5; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer where appropriate, and the State, if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5 and may pose an imminent threat to transportation or national security, or of terrorism. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of an HME;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1515.5(h); and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) TSA serves a Final Determination of Threat Assessment on the State in which the applicant applied for the HME, the applicant's employer where appropriate, and on the applicant, if the appeal of the Initial Determination results in a finding that the applicant poses a security threat.

(5) TSA serves a Withdrawal of the Initial Determination of Threat Assessment or a Withdrawal of Final Determination of Threat Assessment on the applicant, and a Determination of No Security Threat on the State and the employer if appropriate, if the appeal results in a finding that the applicant does not pose a security threat, or if TSA grants the applicant a waiver pursuant to § 1515.7.

§ 1572.17 Applicant information required for TWIC security threat assessment.

An applicant must supply the information required in this section, in a form acceptable to TSA, when applying to obtain or renew a TWIC.

(a) The applicant must provide the following identifying information:

(1) Legal name, including first, middle, and last; any applicable suffix; and any other name used previously.

(2) Current and previous mailing address, current residential address if it differs from the current mailing address, and email address if available.

(3) Date of birth.

(4) Social security number. Providing the social security number is voluntary; however, failure to provide it will delay and may prevent completion of the threat assessment.

(5) Gender.

(6) Height, weight, hair color, and eye color.

(7) City, state, and country of birth.

(8) Immigration status and, if the applicant is a naturalized citizen of the United States, the date of naturalization.

(9) Alien registration number, if applicable.

(10) The reason that the applicant requires a TWIC, including the applicant's job description and the primary facility, vessel, or port location(s) where the applicant will most likely require unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(11) The name, telephone number, and address of the applicant's current employer(s), if working for the employer requires a TWIC. An applicant whose current employer does not require possession of a TWIC, does not have a single employer, or is self-employed, must provide the primary vessel or port location(s) where the applicant requires unescorted access, if known. This statement does not limit access to other facilities, vessels, or ports, but establishes eligibility for a TWIC.

(b) The applicant must provide a statement, signature, and date of signature that he or she--

(1) Was not convicted, or found not guilty by reason of insanity, of a disqualifying crime listed in § 1572.103(b), in a civilian or military jurisdiction, during the seven years before the date of the application;

(2) Was not released from incarceration, in a civilian or military jurisdiction, for committing a disqualifying crime listed in § 1572.103(b), during the five years before the date of the application;

(3) Is not wanted, or under indictment, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in § 1572.103;

(4) Was not convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense identified in § 1572.103(a), in a civilian or military jurisdiction;

(5) Has not been adjudicated as lacking mental capacity, or committed to a mental health facility involuntarily;

(6) Meets the immigration status requirements described in § 1572.105;

(7) Has, or has not, served in the military, and if so, the branch in which he or she served, the date of discharge, and the type of discharge; and

(8) Has been informed that Federal regulations under § 1572.19 impose a continuing obligation on the TWIC holder to disclose to TSA if he or she is convicted, or found not guilty by reason of insanity, of a disqualifying crime, adjudicated as lacking mental capacity, or committed to a mental health facility.

(c) Applicants, applying to obtain or renew a TWIC, must submit biometric information to be used for identity verification purposes. If an individual cannot provide the selected biometric, TSA will collect an alternative biometric identifier.

(d) The applicant must certify and date receipt the following statement:

Privacy Act Notice: Authority: The authority for collecting this information is 49 U.S.C. 114, 40113, and 5103a. **Purpose:** This information is needed to verify your identity and to conduct a security threat assessment to evaluate your suitability for a Transportation Worker Identification Credential. Furnishing this information, including your SSN or alien registration number, is voluntary; however, failure to provide it will delay and may prevent completion of your security threat assessment. **Routine Uses:** Routine uses of this information include disclosure to the FBI to retrieve your criminal history record; to TSA contractors or other agents who are providing services relating to the security threat assessments; to appropriate governmental agencies for licensing, law enforcement, or security purposes, or in the interests of national security; and to foreign and international governmental authorities in accordance with law and international agreement.

(f) The applicant must certify the following statement in writing:

As part of my employment duties, I am required to have unescorted access to secure areas of maritime facilities or vessels in which a Transportation Worker Identification Credential is required; or I am now, or I am applying to be, a credentialed merchant mariner.

(g) The applicant must certify and date receipt the following statement, immediately before the signature line:

The information I have provided on this application is true, complete, and correct, to the best of my knowledge and belief, and is provided in good faith. I understand that a knowing and willful false statement, or an omission of a material fact on this application, can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code), and may be grounds for denial of a Transportation Worker Identification Credential.

(h) The applicant must certify the following statement in writing:

I acknowledge that if the Transportation Security Administration determines that I pose a security threat, my employer, as listed on this application, may be notified.

§ 1572.19 Applicant responsibilities for a TWIC security threat assessment.

(a) Implementation schedule. Except as provided in paragraph (b) of this section, applicants must provide the information required in § 1572.17, when so directed by the owner/operator and consistent with Figure 1 below. The Group Numbers are listed in Figure 1.

Figure 1-Title

	Start Date	End Date
Group 1	Effective date of rule.	Not later than 10 months after effective date of rule, unless otherwise authorized by TSA.
Group 2	After Group 1	Not later than 15 months after effective date of rule, unless otherwise authorized by TSA.
Group 3	After Group 2	Not later than 18 months after effective date of rule, unless otherwise authorized by TSA.

(b) Implementation schedule for certain mariners. An applicant, who holds a Merchant Mariner Document (MMD) issued after February 3, 2003, and before the [Insert effective date of this rule], or a Merchant Marine License (License) issued after January 13, 2006, and before [Insert the effective date of this rule], must submit the information required in this section, but is not required to undergo the security threat assessment described in this part.

(c) Surrender of TWIC. If an individual is disqualified from holding a TWIC under §1572.5, he or she must surrender the TWIC to TSA. Failure to surrender the TWIC to TSA may result in immediate revocation under § 1572.5(b) and/or civil penalties.

(d) Continuing responsibilities. An individual who holds a TWIC must surrender the TWIC, as required in paragraph (a) of this section, within 24 hours if the individual--

(1) Is convicted of, wanted, under indictment or complaint, or found not guilty by reason of insanity, in a civilian or military jurisdiction, for a disqualifying criminal offense identified in § 1572.103; or

(2) Is adjudicated as lacking mental capacity or committed to a mental health facility, as described in § 1572.109; or

(3) Renounces or loses U.S. citizenship or status as a lawful permanent resident; or

(4) Violates his or her immigration status and/or is ordered removed from the United States.

(e) Submission of fingerprints and information. (1) TWIC applicants must submit fingerprints and the information required in § 1572.17, in a form acceptable to TSA, to obtain or renew a TWIC.

(2) When submitting fingerprints and the information required in § 1572.17, the fee required in § 1572.503 must be remitted to TSA.

(f) Lost or stolen credentials. If a TWIC holder loses possession of the credential, he or she must notify TSA immediately.

§ 1572.21 Procedures for TWIC security threat assessment.

(a) Contents of security threat assessment. The security threat assessment TSA conducts includes a fingerprint-based criminal history records check, an intelligence-related check, and a final disposition.

(b) Fingerprint-based check. The following procedures must be completed to conduct a fingerprint-based criminal history records check:

(1) Consistent with the implementation schedule described in § 1572.19(a) and (b), and as required in 33 CFR 104.200, 105.200, or 106.200, applicants are notified

(2) During enrollment, TSA—

(i) Collects fingerprints, applicant information, and the fee required in § 1572.17;

(ii) Transmits the fingerprints to the FBI/CJIS in accordance with the FBI/CJIS fingerprint submission standards.

(iii) Receives and adjudicates the results of the check from FBI/CJIS, in accordance with § 1572.103 and, if applicable, § 1572.107.

(c) Intelligence-related check. To conduct an intelligence-related check, TSA completes the following procedures:

(1) Reviews the applicant information required in § 1572.17;

(2) Searches domestic and international Government databases required to determine if the applicant meets the requirements of §§ 1572.105, 1572.107, and 1572.109;

(3) Adjudicates the results of the check in accordance with §§ 1572.103, 1572.105, 1572.107, and 1572.109.

(d) Final disposition. Following completion of the procedures described in paragraphs (b) and/or (c) of this section, the following procedures apply, as appropriate:

(1) TSA serves a Determination of No Security Threat on the applicant if TSA determines that the applicant meets the security threat assessment standards described in § 1572.5. In the case of a mariner, TSA also serves a Determination of No Security Threat on the Coast Guard.

(2) TSA serves an Initial Determination of Threat Assessment on the applicant if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5. The Initial Determination of Threat Assessment includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting denial of the TWIC;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1515.5; and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination, or does not request an extension of time within 60 days of receipt of the Initial Determination in order to file an appeal, the Initial Determination becomes a Final Determination of Security Threat Assessment.

(3) TSA serves an Initial Determination of Threat Assessment and Immediate Revocation on the applicant, the applicant's employer where appropriate, the FMSC, and in the case of a mariner applying for a TWIC, on the Coast Guard, if TSA determines that the applicant does not meet the security threat assessment standards described in § 1572.5 and may pose an imminent security threat. The Initial Determination of Threat Assessment and Immediate Revocation includes—

(i) A statement that TSA has determined that the applicant poses a security threat warranting immediate revocation of a TWIC and unescorted access to secure areas;

(ii) The basis for the determination;

(iii) Information about how the applicant may appeal the determination, as described in § 1515.5(h); and

(iv) A statement that if the applicant chooses not to appeal TSA's determination within 60 days of receipt of the Initial Determination and Immediate Revocation, the Initial Determination and Immediate Revocation becomes a Final Determination of Threat Assessment.

(4) TSA serves a Final Determination of Threat Assessment on the applicant, the applicant's employer where appropriate, the FMSC, and in the case of a mariner applying for a TWIC, on the Coast Guard, if the appeal of the Initial Determination results in a finding that the applicant poses a security threat.

(5) TSA serves a Withdrawal of the Initial Determination of Threat Assessment on the applicant. TSA serves a Withdrawal of Final Determination of Threat Assessment or a Determination of No Security Threat on the applicant, the applicant's employer where appropriate, and in the case of a mariner applying for a TWIC, the Coast Guard, if the appeal results in a finding that the applicant does not pose a security threat, or if TSA grants the applicant a waiver pursuant to § 1515.7.

(e) Expiration date for a TWIC. A TWIC expires five years after it was issued, at the end of the month in which it was issued.

§ 1572.23 Conforming equipment; Incorporation by reference.

Each owner/operator required to have access control systems and equipment, including card readers, in conjunction with TWIC, must meet TSA-approved standards. The standards are set forth in FIPS-201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors, March, 2006, by the National Institute of Standards and Technology, U.S. Department of Commerce; Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.3, 2006, by the Physical

Access Interagency Interoperability Working Group, approved by the Government Smart Card Interagency Advisory Board; and the TWIC Smart Card Reader Specification, Version 0.6, August 25, 2005. TSA plans to incorporate these standards by reference in the final rule. The Director of the Federal Register approves this incorporation by reference in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain copies from the Credentialing Program Office (Attn: TWIC Program), TSA-19, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; e-mail: credentialing@dhs.gov. You may inspect or make copies at: (1) TSA's Docket No. TSA-2006-24191, at http://dms.dot.gov, or by visiting the Docket Management Facility, U.S. Department of Transportation, Room Plaza 401, 400 Seventh Street SW, Washington, DC 20590-0001; (2) Accessing the "Industry Standards of TWIC" portion of the Industry Partners/TSA Pilots & Programs section of TSA's Web site at http://www.tsa.gov/public/; or (3) at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202-741-6030, or go to http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html .

§ 1572.24-1572.40 [Reserved]

§ 1572.41 Compliance, inspection, and enforcement.

(a) Each owner/operator must allow TSA, at any time or place, to make any inspections or tests, including copying records, to determine compliance of an owner/operator with—

(1) This subchapter and part 1520 of this chapter; and

(2) 46 U.S.C. 70105 and 49 U.S.C. 114.

(b) At the request of TSA, each owner/operator must provide evidence of compliance with this part, including copies of records.

Subpart B--Qualification Standards for Security Threat Assessments

§ 1572.101 Scope.

This subpart applies to applicants who hold or are applying to obtain, renew, or transfer an HME or TWIC. Applicants for an HME are subject to safety requirements issued by the Federal Motor Carrier Safety Administration under 49 CFR part 383 and by the State issuing the HME, including additional immigration status and criminal history standards.

§ 1572.103 Disqualifying criminal offenses.

(a) Permanent disqualifying criminal offenses. An applicant has a permanent disqualifying offense, if convicted, or found not guilty by reason of insanity, in a civilian or military jurisdiction of any of the following felonies:

(1) Espionage or conspiracy to commit espionage.

(2) Sedition, or conspiracy to commit sedition.

(3) Treason, or conspiracy to commit treason.

(4) A crime listed in 18 U.S.C. Chapter 113B—Terrorism, or a State law that is comparable, or conspiracy to commit such crime.

(5) A crime involving a transportation security incident. A transportation security incident is a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area, as defined in 46 U.S.C. 70101. A work stoppage, or other nonviolent employee-related

action, resulting from an employer-employee dispute is not a transportation security incident.

(6) Improper transportation of a hazardous material under 49 U.S.C. 5124, or a State law that is comparable.

(7) Unlawful possession, use, sale, distribution, manufacture, purchase, receipt, transfer, shipping, transporting, import, export, storage of, or dealing in an explosive or explosive device. An explosive or explosive device includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j); and a destructive device, as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).

(8) Murder.

(9) Conspiracy or attempt to commit the crimes in paragraphs (a)(5)-(a)(8).

(10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq., or a State law that is comparable, where one of the predicate acts found by a jury or admitted by the defendant, consists of one of the offenses listed in paragraphs (a)(4) or (a)(8) of this section.

(b) Interim disqualifying criminal offenses. The felonies listed in paragraphs (b)(1) through (b)(14) of this section are disqualifying, if either the applicant was convicted, or found not guilty by reason of insanity, of the crime in a civilian or military jurisdiction, within the seven years preceding the date of application; or the applicant was released from incarceration for the crime, within the five years preceding the date of application.

(1) Assault with intent to murder.

(2) Kidnapping or hostage taking.

(3) Rape or aggravated sexual abuse.

(4) Unlawful possession, use, sale, manufacture, purchase, distribution, receipt, transfer, shipping, transporting, delivery, import, export of, or dealing in a firearm or other weapon. A firearm or other weapon includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C.5 845(a), or items contained on the U.S. Munitions Import List at 27 CFR 447.21.

(5) Extortion.

(6) Dishonesty, fraud, or misrepresentation, including identity fraud.

(7) Bribery.

(8) Smuggling.

(9) Immigration violations.

(10) Violations of the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. 1961, et seq., or a State law that is comparable, other than the violations listed in paragraph (a)(10) of this section.

(11) Robbery.

(12) Distribution of, possession with intent to distribute, or importation of a controlled substance.

(13) Arson.

(14) Conspiracy or attempt to commit the crimes in this paragraph (b).

(c) Under want or warrant. An applicant who is wanted, or under indictment in any civilian or military jurisdiction for a felony listed in this section, is disqualified until the want or warrant is released.

(d) Determination of arrest status. (1) When a fingerprint-based check discloses an arrest for a disqualifying crime listed in this section without indicating a disposition, TSA will so notify the applicant and provide instructions on how the applicant must clear the disposition, in accordance with paragraph (d)(2) of this section.

(2) The applicant must provide TSA with written proof that the arrest did not result in a disqualifying criminal offense, within 60 days after the service date of the notification in paragraph (d)(1) of this section. If TSA does not receive proof in that time, TSA will notify the applicant that he or she is disqualified. In the case of an HME, TSA will notify the State that the applicant is disqualified, and in the case of a mariner applying for TWIC, TSA will notify the Coast Guard that the applicant is disqualified.

§ 1572.105 Immigration status.

(a) An applicant applying for a security threat assessment for a TWIC or HME must be—

(1) A citizen of the United States who has not renounced or lost his or her U.S. citizenship;

(2) A lawful permanent resident of the United States, as defined in § 101(a)(20) of the Immigration and Nationality Act (8 U.S.C. 1101); or

(3) An individual who is-–

(i) In lawful nonimmigrant status, and possesses valid evidence of unrestricted employment authorization;

(ii) A refugee admitted under 8 U.S.C. 1157, and possessing valid evidence of unrestricted employment authorization;

(iii) An alien granted asylum under 8 U.S.C. 1158, and possessing valid evidence of unrestricted employment authorization; or

(iv) A commercial driver licensed by Canada or Mexico, who is admitted to the United States, under 8 CFR 214.2(b)(4)(i)(E), to conduct business in the United States.

(b) To determine an applicant's immigration status, TSA checks relevant Federal databases and may perform other checks, including verifying the validity of the applicant's social security number or alien registration number.

§ 1572.107 Other analyses.

(a) TSA checks the following databases, and analyzes the resulting information, to determine whether applicant poses a security threat:

(1) Interpol and other international databases, as appropriate.

(2) Terrorist watchlists and related databases.

(3) Any other databases relevant to determining whether an applicant poses, or is suspected of posing, a security threat, or that confirm an applicant's identity.

(b) TSA may determine that an applicant poses a security threat, if the search conducted under this part reveals extensive foreign or domestic criminal convictions, a conviction for a serious crime not listed in § 1572.103, or a period of foreign or domestic imprisonment that exceeds 365 consecutive days.

§ 1572.109 Mental incapacity.

(a) An applicant has mental incapacity, if he or she has been—

(1) Adjudicated as lacking mental capacity; or

(2) Committed to a mental health facility.

(b) An applicant is adjudicated as lacking mental capacity, if—

(1) A court, board, commission, or other lawful authority has determined that the applicant, as a result of marked subnormal intelligence, mental illness, incompetence, condition, or disease, is a danger to him- or herself or others, or lacks the mental capacity to conduct or manage his or her own affairs.

(2) This includes a finding of insanity by a court in a criminal case and a finding of incompetence to stand trial; or a finding of not guilty by reason of lack of mental responsibility, by any court, or pursuant to articles 50a and 76b of the Uniform Code of Military Justice (10 U.S.C. 850a and 876b).

(c) An applicant is committed to a mental health facility, if he or she is formally committed to a mental health facility by a court, board, commission, or other lawful authority, including involuntary commitment and commitment for lacking mental capacity, mental illness, and drug use. This does not include commitment to a mental health facility for observation or voluntary admission to a mental health facility.

§§ 1572.111-1572.139 [Reserved]

Subpart C--Transportation of Explosives from Canada to the United States

§ 1572.201 Via commercial motor vehicle**.**

(a) Applicability. This section applies to carriers that carry explosives from Canada to the United States, using a driver who is not a U.S. citizen or lawful permanent resident alien of the United States.

(b) Terms used in this section. For purposes of this section:

Carrier means any “motor carrier” or “motor private carrier”, as defined in 49 U.S.C. 13102(12) and (13), respectively.

Customs Service means the U.S. Customs Service.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known driver means a driver of a motor vehicle who has been determined by the Governments of Canada and the United States to present no known security concern.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Lawful permanent resident alien means a lawful permanent resident alien of the United States, as defined by 8 U.S.C. 1101(a)(2).

Offeror means the person offering a shipment to the carrier for transportation from Canada to the United States, and may also be known as the "consignor" in Canada.

(c) Prior approval of carrier, offeror, and driver. (1) No carrier may transport in commerce any explosive into the United States from Canada via motor vehicle, if the driver of the vehicle is a not a U. S. citizen or lawful permanent resident alien, unless the carrier, offeror, and driver are identified on a TSA list as a known carrier, known offeror, and known driver, respectively.

(2) The carrier must ensure that it, its offeror, and its driver have been determined to be a known carrier, known offeror, and known driver, respectively. If any has not

been so determined, the carrier must submit the following information to Transport Canada:

(i) The carrier must provide its--

(A) Official name;

(B) Business number;

(C) Any trade names; and

(D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

(A) Official name.

(B) Business number.

(C) Address.

(iii) The following information about any driver the carrier may use to transport explosives into the United States from Canada, who is neither a U.S. citizen nor lawful permanent resident alien of the United States:

(A) Full name.

(B) Canada Commercial Driver's License number.

(C) Both current and most recent prior residential addresses.

(3) Transport Canada will determine that the carrier and offeror are legitimately doing business in Canada, and will also determine that the drivers are properly licensed and present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known carriers, offerors, and drivers and their identifying information.

(4) TSA will update and maintain the list of known carriers, offerors, and drivers and forward the list to the Customs Service.

(5) Once included on the list, the carriers, offerors, and drivers need not obtain prior approval for future transport of explosives under this section.

(d) TSA checks. TSA may periodically check the data on the carriers, offerors, and drivers to confirm their continued eligibility, and may remove from the list any that TSA determines is not known or is a threat to security.

(e) At the border. (1) Driver who is not a U.S. citizen or lawful permanent resident alien. Upon arrival at the border, and prior to entry into the United States, the driver must provide a valid Canadian commercial driver's license to the Customs Service.

(2) Driver who is a U.S. citizen or lawful permanent resident alien. If the Customs Service cannot verify that the driver is on the list, and if the driver is a U.S. citizen or lawful permanent resident alien, the driver may be cleared by the Customs Service upon providing--

(i) A valid U.S. passport; or

(ii) One or more other document(s), including a form of U.S. Federal or State Government-issued identification with photograph, acceptable to the Customs Service.

(3) Compliance. If a carrier attempts to enter the United States without having complied with this section, the Customs Service will deny entry of the explosives and may take other appropriate action.

§ 1572.203 Via railroad carrier.

(a) Applicability. This section applies to railroad carriers that carry explosives from Canada to the United States, using a train crew member who is not a U.S. citizen or lawful permanent resident alien of the United States.

(b) Terms under this section. For purposes of this section:

Customs Service means the U.S. Customs Service.

Explosive means a material that has been examined by the Associate Administrator for Hazardous Materials Safety, Research and Special Programs Administration, in accordance with 49 CFR 173.56, and determined to meet the definition for a Class 1 material in 49 CFR 173.50.

Known railroad carrier means a person that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known offeror means an offeror that has been determined by the Governments of Canada and the United States to be a legitimate business, operating in accordance with all applicable laws and regulations governing the transportation of explosives.

Known train crew member means an individual used to transport explosives from Canada to the United States, who has been determined by the Governments of Canada and the United States to present no known security concern.

Lawful permanent resident alien means a lawful permanent resident alien of the United States, as defined by 8 U.S.C. 1101(a)(2).

Offeror means the person offering a shipment to the railroad carrier for transportation from Canada to the United States, and may also be known as the "consignor" in Canada.

Railroad carrier means "railroad carrier", as defined in 49 U.S.C. 20102.

(c) Prior approval of railroad carrier, offeror, and train crew member. (1) No railroad carrier may transport in commerce any explosive into the United States from Canada, via a train operated by a crew member who is not a U.S. citizen or lawful permanent resident alien, unless the railroad carrier, offeror, and train crew member are identified on a TSA list as a known railroad carrier, known offeror, and known train crew member, respectively.

(2) The railroad carrier must ensure that it, its offeror, and each of its crew members have been determined to be a known railroad carrier, known offeror, and known train crew member, respectively. If any has not been so determined, the railroad carrier must submit the following information to Transport Canada:

(i) The railroad carrier must provide its--

(A) Official name;

(B) Business number;

(C) Any trade names; and

(D) Address.

(ii) The following information about any offeror of explosives whose shipments it will carry:

(A) Official name.

(B) Business number.

(C) Address.

(iii) The following information about any train crew member the railroad carrier may use to transport explosives into the United States from Canada, who is neither a U.S. citizen nor lawful permanent resident alien:

(A) Full name.

(B) Both current and most recent prior residential addresses.

(3) Transport Canada will determine that the railroad carrier and offeror are legitimately doing business in Canada and will also determine that the train crew members present no known problems for purposes of this section. Transport Canada will notify TSA of these determinations by forwarding to TSA lists of known railroad carriers, offerors, and train crew members and their identifying information.

(4) TSA will update and maintain the list of known railroad carriers, offerors, and train crew members and forward the list to the Customs Service.

(5) Once included on the list, the railroad carriers, offerors, and train crew members need not obtain prior approval for future transport of explosives under this section.

(d) TSA checks. TSA may periodically check the data on the railroad carriers, offerors, and train crew members to confirm their continued eligibility, and may remove from the list any that TSA determines is not known or is a threat to security.

(e) At the border. (1) Train crew members who are not U.S. citizens or lawful permanent resident aliens. Upon arrival at a point designated by the Customs Service for inspection of trains crossing into the United States, the train crew members of a train transporting explosives must provide sufficient identification to the Customs Service to

enable that agency to determine if each crew member is on the list of known train crew members maintained by TSA.

(2) Train crew members who are U.S. citizens or lawful permanent resident aliens. If the Customs Service cannot verify that the crew member is on the list and the crew member is a U.S. citizen or lawful permanent resident alien, the crew member may be cleared by the Customs Service upon providing--

(i) A valid U.S. passport; or

(ii) One or more other document(s), including a form of U.S. Federal or state Government-issued identification with photograph, acceptable to the Customs Service.

(3) Compliance. If a carrier attempts to enter the U.S. without having complied with this section, the Customs Service will deny entry of the explosives and may take other appropriate action.

Subpart D [Reserved]

Subpart E—Fees for Security Threat Assessments for Hazmat Drivers

§ 1572.400 Scope and definitions.

(a) Scope. This part applies to--

(1) States that issue an HME for a commercial driver's license;

(2) Individuals who apply to obtain or renew an HME for a commercial driver's license and must undergo a security threat assessment under 49 CFR part 1572; and

(3) Entities who collect fees from such individuals on behalf of TSA.

(b) Terms. As used in this part:

Commercial driver's license (CDL) is used as defined in 49 CFR 383.5.

Day means calendar day.

FBI Fee means the fee required for the cost of the Federal Bureau of Investigation (FBI) to process fingerprint identification records and name checks.

Information Collection Fee means the fee required, in this part, for the cost of collecting and transmitting fingerprints and other applicant information under 49 CFR part 1572.

Threat Assessment Fee means the fee required, in this part, for the cost of TSA adjudicating security threat assessments, appeals, and waivers under 49 CFR part 1572.

TSA agent means an entity approved by TSA to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572, and fees in accordance with this part.

§ 1572.401 Fee collection options.

(a) State collection and transmission. If a State collects fingerprints and applicant information under 49 CFR part 1572, the State must collect and transmit to TSA the Threat Assessment Fee, in accordance with the requirements of § 1572.403. The State also must collect and remit the FBI Fee, in accordance with established procedures.

(b) TSA agent collection and transmission. If a TSA agent collects fingerprints and applicant information under 49 CFR part 1572, the agent must—

(1) Collect the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in accordance with procedures approved by TSA;

(2) Transmit to TSA the Threat Assessment Fee, in accordance with procedures approved by TSA; and

(3) Transmit to TSA the FBI Fee, in accordance with procedures approved by TSA and the FBI.

§ 1572.403 Procedures for collection by States.

This section describes the procedures that a State, which collects fingerprints and applicant information under 49 CFR part 1572; and the procedures an individual who applies to obtain or renew an HME, for a CDL in that State, must follow for collection and transmission of the Threat Assessment Fee and the FBI Fee.

(a) Imposition of fees. (1) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(2) The following FBI Fee is required for the FBI to process fingerprint identification records and name checks required under 49 CFR part 1572: the fee collected by the FBI under 28 U.S.C. 534.

(3) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the State the Threat Assessment Fee and the FBI Fee, in a form and manner approved by TSA and the State, when the individual submits the application for the HME to the State.

(b) Collection of fees. (1) A State must collect the Threat Assessment Fee and FBI Fee, when an individual submits an application to the State to obtain or renew an HME.

(2) Once TSA receives an application from a State for a security threat assessment under 49 CFR part 1572, the State is liable for the Threat Assessment Fee.

(3) Nothing in this subpart prevents a State from collecting any other fees that a State may impose on an individual who applies to obtain or renew an HME.

(c) Handling of fees. (1) A State must safeguard all Threat Assessment Fees, from the time of collection until remittance to TSA.

(2) All Threat Assessment Fees are held in trust by a State for the beneficial interest of the United States in paying for the costs of conducting the security threat assessment, required by 49 U.S.C. 5103a and 49 CFR part 1572. A State holds neither legal nor equitable interest in the Threat Assessment Fees, except for the right to retain any accrued interest on the principal amounts collected pursuant to this section.

(3) A State must account for Threat Assessment Fees separately, but may commingle such fees with other sources of revenue.

(d) Remittance of fees. (1) TSA will generate and provide an invoice to a State on a monthly basis. The invoice will indicate the total fee dollars (number of applicants times the Threat Assessment Fee) that are due for the month.

(2) A State must remit to TSA full payment for the invoice, within 30 days after TSA sends the invoice.

(3) TSA accepts Threat Assessment Fees only from a State, not from an individual applicant for an HME.

(4) A State may retain any interest that accrues on the principal amounts collected between the date of collection and the date the Threat Assessment Fee is remitted to TSA, in accordance with paragraph (d)(2) of this section.

(5) A State may not retain any portion of the Threat Assessment Fee to offset the costs of collecting, handling, or remitting Threat Assessment Fees.

(6) Threat Assessment Fees, remitted to TSA by a State, must be in U.S. currency and made payable to the "Transportation Security Administration."

(7) Threat Assessment Fees must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(8) TSA will not issue any refunds of Threat Assessment Fees.

(9) If a State does not remit the Threat Assessment Fees for any month, TSA may decline to process any HME applications from that State.

§ 1572.405 Procedures for collection by TSA.

This section describes the procedures that an individual, who applies to obtain or renew an HME for a CDL, must follow if a TSA agent collects and transmits the Information Collection Fee, Threat Assessment Fee, and FBI Fee.

(a) Imposition of fees. (1) The following Information Collection Fee is required for a TSA agent to collect and transmit fingerprints and applicant information, in accordance with 49 CFR part 1572: $38.

(2) The following Threat Assessment Fee is required for TSA to conduct a security threat assessment, under 49 CFR part 1572, for an individual who applies to obtain or renew an HME: $34.

(3) The following FBI Fee is required for the FBI to process fingerprint identification records and name checks required under 49 CFR part 1572: The fee collected by the FBI under 28 U.S.C. 534.

(4) An individual who applies to obtain or renew an HME, or the individual's employer, must remit to the TSA agent the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in a form and manner approved by TSA, when the individual submits the application required under 49 CFR part 1572.

(b) Collection of fees. A TSA agent will collect the fees required under this section, when an individual submits an application to the TSA agent, in accordance with 49 CFR part 1572.

(c) Remittance of fees. (1) Fees required under this section, which are remitted to a TSA agent, must be made in U.S. currency and made payable to the "Transportation Security Administration."

(2) Fees required under this section must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(3) TSA will not issue any refunds of fees required under this section.

(4) Applications, submitted in accordance with 49 CFR part 1572, will be processed only upon receipt of all applicable fees under this section.

Subpart F--Fees for Security Threat Assessments for Transportation Worker Identification Credentials (TWIC)

§ 1572.500 Scope.

This subpart applies to individuals who apply for, or renew, a Transportation Worker Identification Credential and must undergo a security threat assessment under 49 CFR part 1572.

§1572.501 Fee collection.

When TSA collects fingerprints and applicant information under 49 CFR 1572.17, TSA will collect the Information Collection Fee, Threat Assessment Fee, and FBI Fee, in accordance with procedures approved by TSA.

§ 1572.503 Fee procedures for collection by TSA or its agent.

(a) When an individual submits the application, required under 49 CFR 1572.17, to obtain or renew a TWIC, the fee must be remitted to TSA or its approved agent in a form and manner approved by TSA.

(1) The fee to obtain or renew a TWIC, other than for those identified in paragraph (a)(2) of this section, is $95-149, depending on the services provided to the regulated party, plus any increase in the FBI Fee that may be made. This fee is made up of the total of the following component fees:

(i) The Information Collection/Credential Issuance Fee covers the cost for TSA or its agent to enroll applicants and is $45-$65.

(ii) The Threat Assessment/Credential Production Fee covers the cost for TSA or its agent to conduct a security threat assessment and is $50-$62.

(iii) The FBI Fee is collected by the FBI under 28 U.S.C. 534.to process fingerprint identification records and name checks, which is $22, plus any increase that the FBI may make.

(2) The fee to obtain a TWIC when the applicant has undergone a comparable threat assessment in connection with an HME, a FAST card, or other threat assessment, as provided in § 1572.5(d); or holds an MMD or License as provided in § 1572.19(b), is $50. This fee is made up of the Information Collection/Credential Issuance Fee and a reduced fee for the Threat Assessment/Credential Production Fee. Such applicants are not charged the FBI Fee.

(3) The fee to replace a credential that has been lost, stolen, or damaged is $36.

(b) Form of fees.

(1) Fees, required under this section, must be made in U.S. currency, and made payable to the "Transportation Security Administration."

(2) Fees, required under this section, must be remitted by check, money order, wire, or any other payment method acceptable to TSA.

(c) TSA will not issue any refunds of fees required under this section.

(d) Applications, submitted in accordance with 49 CFR 1572.17, will be processed only upon receipt of all applicable fees.

(e) The fees prescribed in paragraphs (a)(1)(i) and (a)(1)(ii) of this section may be adjusted annually on or after October 1, 2007, by publication of an inflation adjustment. A notice in the Federal Register will announce the inflation adjustment. The adjustment shall be a composite of the Federal civilian pay raise assumption and non-pay inflation factor for that fiscal year issued by the Office of Management and Budget for agency use in implementing OMB Circular A-76, weighted by the pay and non-pay proportions of total funding for that fiscal year. If Congress enacts a different Federal civilian pay raise percentage than the percentage issued by OMB for Circular A-76, the Department of Homeland Security may adjust the fees to reflect the enacted level. The required fee shall be the amount prescribed in paragraphs (a)(1)(i) and (a)(1)(ii), plus the latest inflation adjustment.

(f) Any FBI Fee amendment that increases or decreases its fees to process fingerprint identification records and name checks will apply to the FBI fees identified in this regulation effective on the date of the FBI increase or decrease.

Dated: MAY 10 2006

Admiral Thomas H. Collins,
Commandant,
United States Coast Guard.

Kip Hawley,
Assistant Secretary,
Transportation Security Administration.

Kas
5-10-06